IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 21 July 2023, accepted 11 August 2023, date of publication 21 August 2023, date of current version 7 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3307139

RESEARCH ARTICLE

Research on Optimal Selection Measurement of DNS Root Instance

ZIJUN LI, CHAO LI, GUOYING SUN, ZHAOXIN ZHANG, YANAN CHENG, AND MUXIN WENG
Harbin Institute of Technology, Harbin 150001, China

Corresponding authors: Zhaoxin Zhang (zhangzhaoxin@hit.edu.cn) and Yanan Cheng (chengyn@hit.edu.cn)

This work was supported in part by the Natural Science Foundation of Shandong Province under Grant ZR2020KF009, and in part by the Young Teacher Development Fund of the Harbin Institute of Technology under Grant IDGA10002081.

ABSTRACT DNS root servers are located at the top of the domain name system and are the cornerstone of the Internet. Currently, root servers deploy numerous root instances using anycast technology. Introducing root instances can improve the parsing performance of root servers and the user access experience. However, we found that some root instances do not show optimal performance, and users cannot access the closest root instance when accessing the root instance or even cross-border access. This paper deploys three types of operator detection points in 31 provincial-level administrative regions in mainland China. Each detection point requests the NS record of the top-level domain name from the root instance server introduced in China to obtain the access data of the root instance server hit by domestic users. At the same time, we propose two methods to determine whether users have achieved the optimal choice of root instance, including the method based on the shortest AS path and the method based on geographical distance. In these two methods, we analyze the optimal selection of root instances for each root server. Finally, we analyze the cross-border access of users and find that China Telecom users are more likely to access the root instance across borders.

INDEX TERMS Cross-border access, DNS, optimal choice, root instance.

I. INTRODUCTION

The Domain Name System (DNS), one of the most critical infrastructures on the Internet, is responsible for mapping domain names and IPs [1]. Its tree-like structure includes root name servers, top-level name servers, authoritative name servers, and local name servers from top to bottom. The root name servers are at the top and act as the cornerstone of Internet operation, the primary carrier to secure Internet applications. Currently, there are 13 root servers worldwide [2]. To relieve the resolution pressure on the root servers, improve the resolution capability and Internet access experience in all regions of the world, as well as reduce DNS attacks [3], [4], [5], the 13 root servers deploy a large number of root instances using anycast [6], [21], [26]. All root servers update the duplicate root zone data files synchronously. The root instance server and its root server use the same IP address and provide the same root resolution service function. As of March 2023, there are 1650 root instances deployed worldwide, among which 6 of the 13 roots (A-1, F-4, I-2, J-3, K-3, L-13) have been introduced in the domestic mainland, with a total of 26 root instances [7]. The number and type of root instances deployed by the six root servers and their geographical locations are shown in Table 1 below.

Although the introduction of root instances can bring many conveniences, at the same time, we find that some root instances do not exhibit optimal performance [23]. We have found such a phenomenon: some users look far away when accessing the root instance and fail to achieve the optimal selection of the root instance [30]. There are root instance nodes that are close to the user, but they actually visit the root instance nodes that are far away and even visit foreign root instance nodes across borders. For example, when domestic telecom users access the I root instance, they all access the I root Tokyo instance and Singapore instance across the border, even though there are I root Beijing and Shenyang instances in China. It not only increases the resolution delay but also reduces the access speed. At the same time, there are

The associate editor coordinating the review of this manuscript and approving it for publication was Paulo Mendes.

TABLE 1. Type and location distribution of introduced root instances in the domestic mainland.

Domestically introduced roots	The number of domestic root instances	Type of the root instance	The geographic location of the root instance
A	1	Global	Guangzhou*1
F	4	Local	Beijing*1,Chongqing*1, Hangzhou*1,Nanning*1
I	2	Global	Beijing*1,Shenyang*1
J	3	Global	Beijing*1,Huzhou*1, Shanghai*1
K	3	Local, Global	Beijing*1,Guangzhou*, Guiyang (Global) *1
L	13	Global	Beijing*4,Changsha*1, Haikou*1,Shanghai*1, Wuhan*2,Xining*2, Zhengzhou*2

certain security risks for users to access the root instance node across borders. In addition, from the operators' perspective, we found that to reduce the traffic settlement between operators, some operators made the introduced root instance only serve the local network or even the local province and could not maximize the service utility. Currently, many researchers have studied root instances. Zhang et al. studied the service range of domestic mainland root instances and found that the service range of some root instances is limited due to the limitation of BGP routing [14]. Lee X et al. studied the problem of DNS root server deployment. They found that the main reason for root zone file distribution delay and BGP routing convergence costs was the unbalanced deployment of 13 root servers [16]. Moura et al. proposed that observing TCP handshakes can continuously measure DNS latency in real-time and achieve good coverage of users [13]. Most studies have focused on measuring the service range of root servers, resolution latency, and root server deployment issues. In contrast, fewer studies have addressed the optimal selection of root instances and cross-border access situations.

Therefore, studying the optimal selection of root instances and cross-border access for users will help to grasp the actual operation status of root instances and provide some references for root server management organizations to optimize the deployment of root instances so that root instances can perform at their best performance. At the same time, operator managers can use this to optimize their operating strategies, strengthen connections with other operators, and optimize users' Internet access experience. In this paper, to study the optimal selection of the root instance and the cross-border access of users, we deploy the three significant operators' probing sites in 31 provinces in a distributed manner. We actively request NS records of all TLDs from the six root servers introduced in the domestic mainland and analyze them for their response packets. The primary contributions are as follows:

- We have deployed 86 probes, including three operators, China Mobile, China Unicom, and China Telecom. These probe sites cover 31 provinces in China except Hong Kong, Macau, and Taiwan.
- In this paper, we present two methods for determining the optimal choice of root instance, by which we can effectively determine whether the user has achieved the optimal choice of root instance. Method one is based on the shortest AS path to judge. The key of the method is to analyze whether the actual AS path is the optimal AS path. We combine the Traceroute path and BGP [25] routing correlation analysis to get the actual AS path from the user to the root instance. The shortest AS path between the probe point and the root server is also obtained. The two are compared, and if the paths are consistent, the user achieves the optimal choice of the root instance server.
- Method two is based on the geographic distance to determine. By locating the root instance to a geographic location, such as Beijing, China, we can infer which root instance is closest to the user. Thus, from the geographical location, we analyze whether the user is accessing the root instance that is closest to him or her.
- Finally, we conducted a detailed analysis of users' cross-border access to the root instance based on the data obtained from the probe. Meanwhile, a brief analysis of the reasons for users' cross-border access is also presented.

The structure of this paper is as follows: Part II introduces the research work related to root instance; Part III introduces the determination method of optimal selection of root instance; Part IV presents the research results; Part V concludes the whole paper.

II. RELATED WORK

A. THE STUDY OF ANYCAST TECHNOLOGY

S. Sarat et al. studied the effect of anycast technology. They selected four top-level domain name servers to analyze the influence of different anycast configurations on DNS services. They found that the anycast technique can reduce the resolution latency of DNS servers, and up to 80% of queries will be selected on the nearest root instance by the anycast technique [8]. Liu et al. captured DNS traffic from C, F, and K root instances and studied how the anycast technique serves global users. They determined whether users accessed the instance closest to them by examining the geographic distance of each root instance from the user. They noticed that the instances selected by BGP routing were not the geographically closest instances. Also, by examining specific AS paths, they found that local instances appeared to have a disproportionate number of non-local users [9]. Li et al. first investigated the anycast technique in terms of both loads balancing as well as geographical proximity. It was found that the root instance node suffers from load imbalance and users querying too far away due to misaligned relationships between domain names and large ISPs as well as misconfigured routes [10]. Bian et al. first proposed using passive

measurements to infer anycast prefixes using collected global BGP routing information and anycast data for analysis. They analyzed the reasons behind the misclassification. The impact of remote peering on path selection was also investigated, and it was found that the invisibility of remote peering when combined with Anycast, tends to impact Anycast performance [11]. Moura et al. first evaluated how IP anycast services cope with pressure. They stress-tested these IP anycast services through public data and found that sites were able to absorb attack traffic with as minor damage as possible. It also investigated how to provide different service levels for different users [12]. Moura et al. proposed that by observing TCP handshakes were able to measure DNS latency continuously and in real-time to achieve good coverage of users. They found that DNS servers can extend their coverage through TCP, and DNS latency estimates for TCP are consistent with UDP latency. Also, this method can be used to detect and correct misconfigurations in BGP routing [13].

B. PERFORMANCE ANALYSIS OF ROOT INSTANCE

Zhang et al. studied the service range of domestic mainland root instances and found that the limitation of BGP routing makes the service range of some root instances limited. They used DNS Censorship to determine whether probe points exist on root instances outside the international gateway that users turn to when querying the root server. In addition, they evaluated the user query performance and the impact of root server selection on the deployment of new root instances [14]. Fan et al. proposed a method to identify and characterize anycast nodes. They combined two methods, CHAOS records and traceroute path information, to identify all the anycast services, and found that the method has 88% accuracy by identifying the F root instance nodes. They also investigated whether the IP addresses of more than 1,000 name servers containing all top-level domains are anycast nodes [15]. Lee et al. studied the problem of DNS root server deployment. They found that the main reason for the delay in the distribution of root zone files and the cost of BGP route convergence was the unbalanced deployment of 13 root servers. They proposed two options to expand the number of root servers, the first option is to deploy global and local root instances hierarchically, and the second option is to geographically spread the root instance nodes all over the world [16]. The performance of root anycast nodes was investigated by Li et al. They analyzed the actual service performance of deployed root anycast nodes in China based on active measurements and found that the service performance of roots with anycast nodes deployed was higher than other roots. In addition, they studied the anomalous resolution of root servers and found that some top-level domains were hijacked [17].

The research in this paper is very different from the previous studies. First, we deploy probing points of different ISPs in each province of the domestic mainland to achieve full coverage of provincial users. Second, we investigate the optimal selection of root instances. Previous research has yet to conduct a detailed study on root instances. We propose two methods to achieve optimal selection determination of root instances, one by the shortest AS path and the other by geographic distance. Finally, we focus on the cross-border access of users and analyze which users are prone to cross-border access to the root instance.

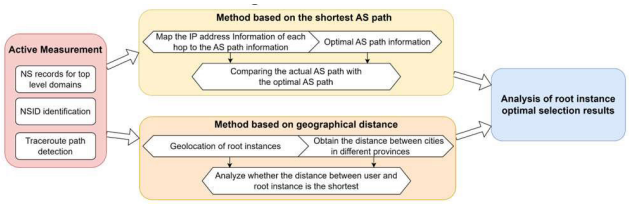

FIGURE 1. Measurement Method Schematic Diagram for Optimal Selection of Root Instances.

III. METHODOLOGY

We describe the methods for data measurement and determining the optimal selection of root instances. Firstly, we obtain data based on probing points. Next, we propose two methods for determining the optimal selection of root instances, including the shortest AS path-based method and the geographical distance-based method. Anycast technology is implemented using the BGP routing protocol. The limited understanding of the network topology by BGP and the ineffective intra-domain routing strategy of ISPs lead to users being unable to select the best root instance, which is not due to the load of the root instance. As a result, this paper assesses the distance between the root server and the user. The process of measuring the optimal selection of root instances is shown in Figure 1.

A. ACTIVE MEASUREMENT

We distribute the detection points of the three major operators (China Mobile, China Unicom, and China Telecom) in 31 provinces, with a total of 86 detection points. The provinces covered by the three detection points are shown in Figure 2. Each detection point sends a DNS query message to the six root servers (A Root, F Root, I Root, J Root, K Root, L Root) that have introduced the root instance in China, requesting to resolve the NS records of 1498 top-level domain names. In the request message, enable the NSID [22] option in the Extended DNS Mechanism (EDNS) to obtain the identification information of the root instance. In the response message, we obtain the result of the NSID field in OPT PSEUDOSECTION and the NS authoritative server information of the top-level domain in the AUTHORITY SECTION. Figure 3 shows the process in that the detection point queries the K root for the NS record of the cn top-level domain and returns the result. It can be seen from the response message that this query is responded to by the "ns1.cn-ggz.k.ripe.net" instance of the K root. Obtaining the NS record and NSID identification information of the top-level domain name is mainly implemented by the DNSPYTHON module in PYTHON. In addition, we obtain the traceroute information between the detection point and the root instance

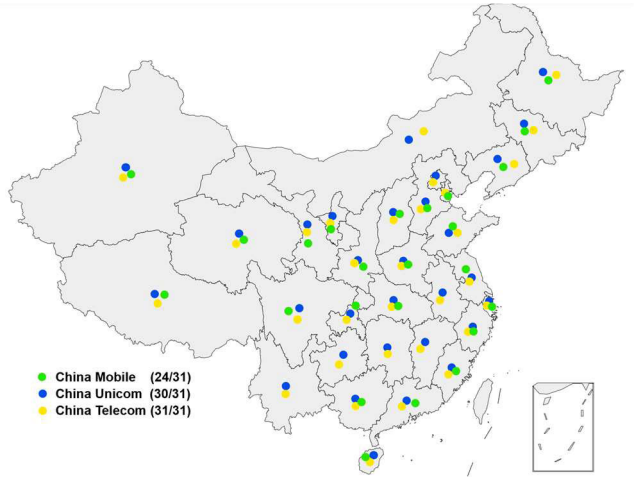

FIGURE 2. Three Operators and Covered Provinces.

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.13 <<>> cn NS +nsid @k.root-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59675
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 11
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; NSID: 6e 73 31 2e 63 6e 2d 67 67 7a 2e 6b 2e 72 69 70 65 2e 6e 65 74 ("ns1.cn-ggz.k.ripe.net")
;; QUESTION SECTION:
;cn.                            IN      NS

;; AUTHORITY SECTION:
cn.                     172800  IN      NS      a.dns.cn.
cn.                     172800  IN      NS      b.dns.cn.
cn.                     172800  IN      NS      c.dns.cn.
cn.                     172800  IN      NS      d.dns.cn.
cn.                     172800  IN      NS      e.dns.cn.
cn.                     172800  IN      NS      f.dns.cn.
cn.                     172800  IN      NS      g.dns.cn.
cn.                     172800  IN      NS      ns.cernet.net.

;; ADDITIONAL SECTION:
a.dns.cn.               172800  IN      A       203.119.25.1
a.dns.cn.               172800  IN      AAAA    2001:dc7::1
b.dns.cn.               172800  IN      A       203.119.26.1
c.dns.cn.               172800  IN      A       203.119.27.1
d.dns.cn.               172800  IN      A       203.119.28.1
d.dns.cn.               172800  IN      AAAA    2001:dc7:1000::1
e.dns.cn.               172800  IN      A       203.119.29.1
f.dns.cn.               172800  IN      A       195.219.8.90
g.dns.cn.               172800  IN      A       66.198.183.65
ns.cernet.net.          172800  IN      A       202.112.0.44

;; Query time: 42 msec
;; SERVER: 193.0.14.129#53(193.0.14.129)
;; WHEN: Thu Jun 15 09:51:48 CST 2023
;; MSG SIZE  rcvd: 383
```

FIGURE 3. The Detection Point Requests the NS Record of the cn Top-level Domain from the K Root.

node, which is used for the geographic location of the root instance.

B. OPTIMAL SELECTION OF ROOT INSTANCES

1) SHORTEST AS PATH-BASED METHOD FOR OPTIMAL SELECTION OF ROOT INSTANCES

We propose a method based on the shortest AS path, which measures the optimal selection of root instances from the perspective of network topology. To determine whether users are accessing the root instance server most optimally, we need to determine whether the current access path is optimal. Only when the actual path taken by the data packet to access the server is consistent with the shortest path that communicates with the network domain can it be considered that the access is done via the optimal path. The difference between the shortest path and the actual access path is illustrated in Figure 4.

As shown in Figure 4, it is easy to see that the green path represents the shortest AS path: AS0 → AS1 → AS3 →

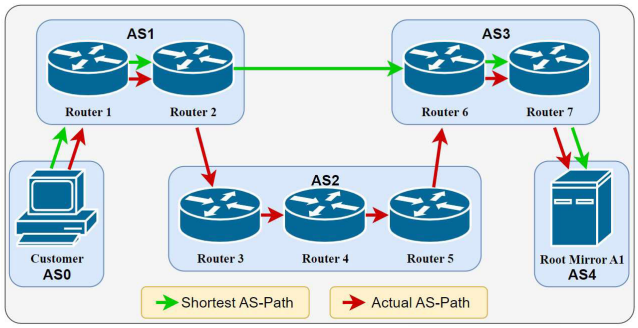

FIGURE 4. Comparison between Shortest and Actual AS-Path.

AS4, whereas the red path is the actual detected path: AS0 → AS1 → AS2 → AS3 → AS4. The possible reasons for this phenomenon are different relationships between ASes, the deliberate configuration of BGP routes by network administrators, congestion of a vast amount of data flows between two ASes, or unreasonable IXP route configurations that prevent ASes that should be interconnected through IXP from accessing each other. The method used in this paper is based on the shortest AS path rather than the shortest routing path because the Internet is volatile and the network conditions are complex. It is difficult to determine which routing path is the most suitable resolving path at the time. In addition, the optimal routing path is affected by multiple factors, such as network packet volume and hop router conditions, making it difficult to have a reference value. The optimal AS path, on the other hand, is relatively stable because the operators of each AS should have configured reliable BGP routes, and the bandwidth and links between each AS domain and its neighbors are relatively high-speed and stable. Therefore, we use the above method to determine whether DNS request packets have taken the optimal AS path [27], including obtaining two types of data: the actual path taken by data packets and the search for the theoretically shortest path.

Obtaining the actual path taken by data packets is relatively simple. Here, the traceroute tool obtains the actual routing path taken by data packets. After obtaining the IP addresses of each router along the routing path, we can look up the IP WHOIS information of each IP address to determine which AS it belongs to.

The tricky part is to discover the true optimal path. Obtaining the shortest path that connects requires more than just a few probes. If IXP route configurations are unreasonable, or if there is some commercial relationship between ASes, we may never be able to discover the shortest AS path from requests of a single probe. In this case, RIPE-ATLAS [18] probe data and extensive data from CAIDA's BGPSTREAM [19] are used for analysis. RIPE-ATLAS probes continuously request TRACEROUTE data from root instance servers, including requests from probes of multiple different operators, which helps expand the dimension of the data and discover possible unreasonable cross-operator request paths. BGPSTREAM's data is collected from massive probes deployed globally by

CAIDA. Each probe requests the AS path within its neighboring ASes daily in a loop, and these probes have various characteristics at different dimensions. Therefore, using this data, we can create an AS connectivity map of a network domain, which enables us to discover the shortest AS path using algorithms such as BFS.

Finally, through a simple comparison, we can discover which AS requests took the long route.

2) GEOGRAPHICAL DISTANCE-BASED METHOD FOR OPTIMAL SELECTION OF ROOT INSTANCES

To analyze the optimal selection of root instances, we propose another method of determining the optimal selection of root instances based on geographical distance. From the perspective of geographical location, we combine the geographical locations of probe points and root instances with the geographical locations of various provinces and cities to analyze the optimal selection of root instances. The specific steps are as follows:

First, based on the active measurement method described in section III-A, we obtain which root instance each probe point accesses. In addition, we obtain the IP address of the root instance, which is the IP address of the nth last hop in the traceroute path, to facilitate the geographical positioning of the root instance in the next step.

Second, we locate the root instance geographically to obtain the geographical location information of the probe points and root instances. This step lays the foundation for analyzing whether users are accessing the nearest root instance when accessing root instances. We first resolve the IP address of the NSID, that is, obtain its A record information. If the IP address can be successfully resolved, the IP is geolocated to obtain the geographic location of the root instance. If the location of the root instance cannot be obtained, we analyze whether there is a string abbreviation of a country and a city in the root instance NSID and determine the geographical location of the root instance according to the string abbreviation. For example, ''ns1.jp-tyo.k.ripe.net'' is the root instance, ''jp'' is the abbreviation of Japan, and ''tyo'' is the three-character code for Tokyo, so the instance is located in Tokyo, Japan. Suppose the NSID does not contain the abbreviation of the country and city. In that case, we use traceroute to obtain the IP address of the last nth hop of the root instance, then use IP positioning to obtain the geographic location information of the root instance.

Third, we obtain a distance table between provinces and cities throughout the country to analyze the distance between users and root instances from the perspective of geographical location.

Finally, by comparing the actual geographical distance between the user and the root instance, we analyze whether there is a better root instance for the user to access nearby. Given the shortest distance, which root instance should the user access the optimal root instance? If there exists one, it means that the user did not achieve the optimal selection of root instances when accessing that root server.

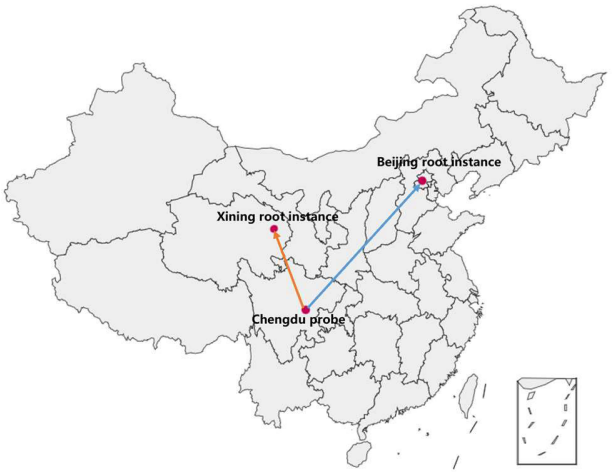

FIGURE 5. An Example of Optimal Selection of Root Instances Based on Geographical Distance. The blue path represents the actual accessed root instance, and the orange path represents the path to the closest root instance. The Chengdu Unicom probing point did not access the nearest Xining root instance but chose the Beijing one.

Consider the scenario in Figure 5, which is taken from a real example in our dataset. During the detection process, we found that when the Chengdu probe point requested the NS record of a top-level domain name from L-root servers, it accessed the root instance labeled ''cn-bjd-aa.'' Through geolocation of the root instance, we know that it is located in Beijing. There are 13 root instances of L root servers domestically, including instances in Beijing, Changsha, Haikou, Shanghai, Wuhan, Xining, and Zhengzhou. According to the distance table calculated from various provinces and cities across the country, we know that among these seven locations, Xining is closest to Chengdu. Therefore, in the best scenario, the Chengdu Unicom probing point should access the Xining root instance of the L root instead of the Beijing instance. It indicates that the Chengdu Unicom probing point did not make an optimal choice when accessing the L root server. Of course, it may be due to BGP route advertisement and enterprise route diversion. However, from the perspective of anycast technology, the Chengdu Unicom probing point should access the closest instance - the Xining root instance.

IV. RESULTS

A. RESULTS OF THE OPTIMAL SELECTION OF ROOT INSTANCES

Currently, six root servers are deployed in China, with different types of root instance deployments, including Global and Local types. Local root instances can only serve the surrounding ASes with a smaller service range [9], [20]. Global root instances can be accessed globally through BGP route advertisement with a broader service range. Therefore, we analyze the optimal selection of Global root instances. In addition, we use the root instance optimal selection rate to illustrate the situation of optimal selection of root instances. That is the rate of optimal selection of root instances = the

TABLE 2. Optimal selection of I root instances.

Operators	Accessed Instance	Rate of optimal selection of root instances
China Mobile	Tokyo instance	1/31
China Unicom	Tokyo instance	0
China Telecom	Tokyo instance, Singapore instance	0

TABLE 3. Optimal selection of J root instances.

Operators	Accessed Instance	Rate of optimal selection of root instances
China Mobile	Beijing instance	17/31
China Unicom	Beijing instance	17/31
China Telecom	Amsterdam instance, Edinburgh instance	0

number of probing points that implement the optimal selection of root instances/total number of provinces. Considering that I Root, J Root, and L Root instances deployed in China are all Global types and have a global service range, we use them as representatives to analyze the optimal selection of root instances.

1) I ROOT

I Root's root instances in mainland China are Global type, with two in Beijing and Shenyang. However, as shown in Table 2, for China Mobile users accessing the I root server, only one province achieved the optimal selection of root instances, namely the user from Beijing who accessed the Beijing instance. All other China Mobile users accessed the Tokyo instance instead of selecting the closer domestic instances. For China Telecom users, the probing point from Shanghai accessed the Singapore instance, whereas users in all other provinces accessed the Tokyo instance. It indicates that these users accessed the I root server across borders and did not implement the optimal selection of root instances. Therefore, the root instance optimal selection rate is 0 for both China Telecom and China Unicom users since they all accessed the instance from Tokyo, Japan, instead of selecting closer domestic instances.

2) J ROOT

J Root server has a total of three domestic instances in China, namely the Beijing instance, the Huzhou instance, and the Shanghai instance. All three instances are Global. Table 3 shows the optimal selection of J Root instances. Overall, the rate of optimal selection of J Root instances is better than that of I Root instances. First, for China Mobile users, the rate of optimal selection reached 17/31, which means that 17 provinces' users achieved optimal selection of root instances when accessing J Root servers. Through probing and analyzing the data, we found that all mobile users access the Beijing instance when accessing J Root. After analyzing the shortest AS path and geographical distance, we identified 17 probing points that achieved optimal selection of root instances by selecting those closer to them. For China Unicom users, similar to China Mobile users, we found they also access the Beijing instance. Therefore, the rate of optimal selection of root instances for China Unicom is also 17/31. As for China Telecom users, we found that all Telecom users accessed the instance across borders. Users from Shanghai accessed two instances in London and Edinburgh, neither of which is a local Shanghai instance. This undoubtedly increases the resolution latency and reduces the service performance of the root instance. Users in the remaining 30 provinces all accessed the Amsterdam instance in the Netherlands without accessing any of the Beijing, Huzhou, or Shanghai instances in China. Therefore, the rate of optimal selection of root instances for China Telecom users is 0. This is related to BGP route announcement and operator route diversion factors.

3) L ROOT

L Root server has 13 root instances in China, distributed in Beijing, Zhengzhou, Wuhan, Shanghai, Changsha, Xining, and Haikou. Table 4 illustrates the optimal selection of L Root instances. Although the more significant number of L Root instances than J Root, the rate of optimal selection of L Root instances is much poorer than that of J Root instances. For China Mobile users, only Urumqi users have access to the Xining instance. Users in all other 30 provinces access the instance from Zhengzhou. Analyzing the shortest AS path and optimal geographical distance, we determined that in the optimal scenario, the Zhengzhou instance should only be accessed by users in Zhengzhou, Taiyuan, and Xi'an. In contrast, users in other provinces have closer root instances available. Xinjiang Urumqi users should indeed access the Xining instance. Therefore, the rate of optimal selection of root instances for China Mobile users is 4/31. For China Unicom users, except for users in Wuhan who access the Wuhan instance, all other users access the Beijing instance. In terms of optimal selection, the ideal scenario would be for the Beijing instance only to be accessed by users in Beijing, Tianjin, Hohhot, Harbin, Changchun, Shenyang, Shijiazhuang, and Jinan. In contrast, users in other provinces have better root instances nearby. For example, Wuhan users should access the Wuhan instance, which is precisely the case. Therefore, the rate of optimal selection of root instances for China Unicom users reached 9/31. As for China Telecom users, the rate of optimal selection of L Root instances, like I Root and J Root, is also 0. Despite having 13 root instances in China, all users in every province are directed abroad to access distant root instances in Sydney, Australia, and Incheon, South Korea. Shanghai Telecom users access the Incheon instance, whereas users in all other provinces access the Sydney instance. At the same time, we found that many domestic L Root instances have yet to serve operators, such as Changsha and Haikou instances, and only Wuhan Unicom

TABLE 4. Optimal selection of L root instances.

Operators	Accessed Instance	Rate of optimal selection of root instances
China Mobile	Zhengzhou instance, Xining instance	4/31
China Unicom	Beijing instance, Wuhan instance	9/31
China Telecom	Sydney instance, Incheon instance	0

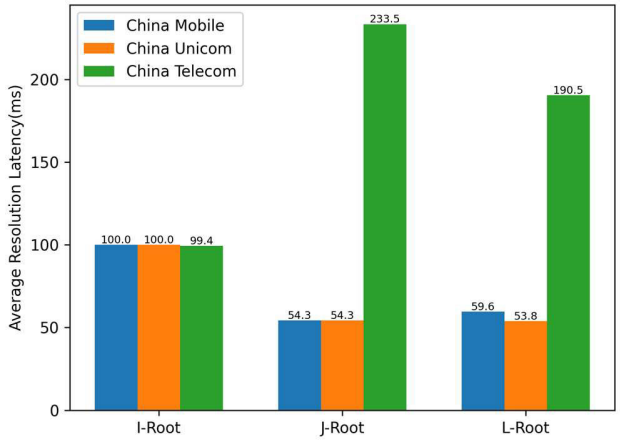

FIGURE 6. Average Resolution Latency for Accessing the Three Root Servers by Different Operators.

users have accessed the Wuhan instance. This is a problem that the root instance management organization needs to pay attention to, as each root instance is deployed using anycast technology and should leverage its technical advantages to allow nearby users to access it.

Analyzing the optimal selection of I, J, and L root instances, we found that J Root instances have a better rate of optimal selection than I and L Root instances. Although L Root has introduced the most significant number of root instances in China, its rate of optimal selection should ideally be the highest, but this is not the case. Figure 6 shows the average resolution latency for accessing the three root servers by different operators' users. From the standpoint of resolution latency, achieving optimal selection of root instances results in a considerably lower resolution latency, such as for J Root's Mobile and Unicom users. In contrast, the resolution latency of Telecom users is approximately four times that of Mobile and Unicom users. Therefore, root server management organizations should optimize the deployment of root instances to enable users to access root instances nearby.

Among the three roots, Telecom users in all 31 provincial administrative regions have a rate of optimal selection for root instances of 0 and have not achieved optimal selection of root instances. It is because these users cross-border access root instances when accessing either I, J, or L Root and do not choose any domestic instance. Considering the serious situation of cross-border access by users, we will analyze in

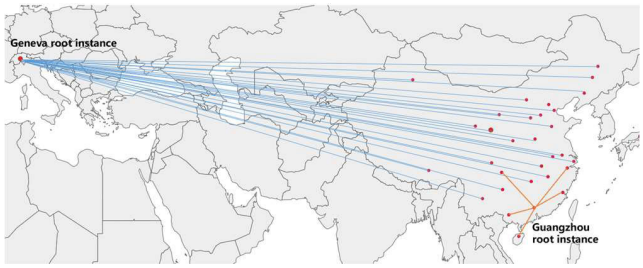

FIGURE 7. Mobile and Unicom Users Accessing the K Root Instance. Blue represents users accessing the root instance across the border; orange represents users accessing the domestic instance.

detail the cross-border access of several roots introduced in China below.

B. CROSS-BORDER ACCESS

From the previous context, we know that Telecom users have all accessed the instances of Root Servers I, J, and L across borders. Therefore, analyzing whether users of the three major operators also have cross-border access when accessing other domestically introduced root servers is necessary. Below, we will conduct a detailed analysis of whether users of K Root have cross-border access.

K Root has deployed three instances in mainland China, located in Beijing, Guangzhou, and Guiyang. Figure 7 shows the situation of Mobile users accessing the K root, revealing that Mobile users in 18 provinces have accessed the Geneva instance, leading to cross-border access to the root instance. The remaining six provinces' Mobile users accessed the nearest Guangzhou instance. For China Unicom users, we found that except for Beijing Unicom users who accessed the Beijing instance, users in the remaining 29 provinces accessed the foreign Geneva instance. For China Telecom users, only Shanghai users accessed the Tokyo instance, whereas the rest accessed the domestically introduced root instances.

Table 5 shows the cross-border access situation of the three operators' users accessing the I, J, K, and L root instances, revealing much outbound traffic from domestic root resolution. Firstly, from the perspective of the root servers, it was found that users had the most severe cross-border access when accessing the I root instance, with a frequency of 100%. Secondly, the K root, especially China Mobile and China Unicom users, had the second most severe cross-border access. The cross-border access situation of J and L roots was the same, with only China Telecom users having cross-border access. Thirdly, from the perspective of the operators, it was found that China Telecom was more prone to cross-border access to the root instances. To reduce inter-operator traffic settlement, telecom operators use routing detours to achieve cross-border access. For example, only China Unicom and China Mobile operator instances were deployed for the I and J roots, so telecom users actively chose to cross borders to avoid inter-operator access. Therefore, large operators should improve the interconnection of root instances and optimize

TABLE 5. Cross-Border access to I, J, K, and L root instances for three types of users.

Operators	I Root	J Root	L Root	K Root
China Mobile	24/24	0	0	19/24
China Unicom	30/30	0	0	29/30
China Telecom	31/31	31/31	31/31	1/31

BGP routing to minimize cross-border access and reduce the security risks brought by cross-border resolution.

V. CONCLUSION

This paper studied the optimal selection of root instances from the users' perspective. We proposed two methods for determining the optimal selection of root instances: based on the shortest AS path and geographic distance. We analyzed the optimal selection situation of root instances for the I, J, and L roots using these two methods. We found that the J root instance had the best optimal selection situation. Additionally, we analyzed the cross-border access situation of users and found that China Telecom users were more likely to have cross-border data access. It is related to factors such as BGP routing announcements and routing detours.

We found that root instance servers' deployment distribution and service scope in various provinces and regions needed to be more balanced. Therefore, it is necessary to strengthen the planning of root instance servers to make domain root resolution services more comprehensive, efficient, and balanced [28], [29]. In addition, to promote the balanced and healthy development of the three major operators' networks, it is also necessary to consider the balance of the deployment of root instances in operator networks. Some operators introduce root instances that only serve their networks, or even their own province's network, meaning that the root instances introduced domestically cannot achieve maximum service utility and need to be optimized. In addition, as many types of root instances as possible should be introduced to improve root instance resolution performance and reduce cross-border access.

This paper focuses on the optimal selection of root instances, which helps root instance management organizations optimize future root instance planning and layout, further enhancing global resolution capabilities and the Internet access experience. However, we mainly studied Global-type instances and did not conduct detailed research on Local-type instances, which is a shortcoming of this article and a key area of future research.

REFERENCES

[1] *Domain Names-Concepts and Facilities*. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc1034

[2] D. Conrad. (2020). *Brief Overview of the Root Server System*. [Online]. Available: https://www.icann.org/en/system/?les/?les/octo-010-06may20-en.pdf

[3] H. S. Hmood, Z. Li, H. K. Abdulwahid, and Y. Zhang, "Adaptive caching approach to prevent DNS cache poisoning attack," *Comput. J.*, vol. 58, no. 4, pp. 973–985, Apr. 2015, doi: 10.1093/comjnl/bxu023.

[4] B. Liu, C. Lu, H. Duan, Y. Liu, Z. Li, S. Hao, and M. Yang, "Who is answering my queries: Understanding and characterizing interception of the DNS resolution path," in *Proc. 27th USENIX Secur. Symp. (USENIX Security)*, 2018, pp. 1113–1128.

[5] B. Saridou, S. Shiaeles, and B. Papadopoulos, "DDoS attack mitigation through root-DNS server: A case study," in *Proc. IEEE World Congr. Services (SERVICES)*, Milan, Italy, Jul. 2019, pp. 60–65, doi: 10.1109/SERVICES.2019.00025.

[6] X. Zhang, T. Sen, Z. Zhang, T. April, B. Chandrasekaran, D. Choffnes, B. M. Maggs, H. Shen, R. K. Sitaraman, and X. Yang, "AnyOpt: Predicting and optimizing IP anycast performance," in *Proc. ACM SIGCOMM Conf.*, Aug. 2021, pp. 447–462.

[7] (2021). *Root Server Technical Operations Association*. [Online]. Available: https://root-servers.org/

[8] S. Sarat, V. Pappas, and A. Terzis, "On the use of anycast in DNS," in *Proc. 15th Int. Conf. Comput. Commun. Netw.*, Arlington, VA, USA, Oct. 2006, pp. 71–78, doi: 10.1109/ICCCN.2006.286248.

[9] Z. Liu, B. Huffaker, M. Fomenkov, N. Brownlee, and K. Claffy, "Two days in the life of the DNS anycast root servers," in *Passive and Active Network Measurement* (Lecture Notes in Computer Science), vol. 4427, S. Uhlig, K. Papagiannaki, and O. Bonaventure, Eds. Berlin, Germany: Springer, 2007, pp. 131–143, doi: 10.1007/978-3-540-71617-4_13.

[10] Z. Li, D. Levin, N. Spring, and B. Bhattacharjee. (2017). *Longitudinal Analysis of Root Server Anycast Inefficiencies*. [Online]. Available: https://zhihao.li/anycast_tr17.pdf

[11] R. Bian, S. Hao, H. Wang, A. Dhamdere, A. Dainotti, and C. Cotton, "Towards passive analysis of anycast in global routing: Unintended impact of remote peering," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 49, no. 3, pp. 18–25, Nov. 2019.

[12] G. C. M. Moura, R. D. O. Schmidt, J. Heidemann, W. B. de Vries, M. Müller, L. Wei, and C. Hesselman, "Anycast vs. DDoS: Evaluating the November 2015 root DNS event," in *Proc. Internet Meas. Conf.*, New York, NY, USA, Nov. 2016, pp. 255–270, doi: 10.1145/2987443.2987446.

[13] G. C. M. Moura, J. Heidemann, W. Hardaker, P. Charnsethikul, J. Bulten, J. M. Ceron, and C. Hesselman, "Old but gold: Prospecting TCP to engineer and live monitor DNS anycast," in *Passive and Active Measurement* (Lecture Notes in Computer Science), vol. 13210, O. Hohlfeld, G. Moura, and C. Pelsser, Eds. Cham, Switzerland: Springer, 2022, doi: 10.1007/978-3-030-98785-5_12.

[14] F. Zhang, C. Lu, B. Liu, H. Duan, and Y. Liu, "Measuring the practical effect of DNS root server instances: A China-wide case study," in *Passive and Active Measurement* (Lecture Notes in Computer Science), vol. 13210, O. Hohlfeld, G. Moura, and C. Pelsser, Eds. Cham, Switzerland: Springer, 2022, pp. 147–159, doi: 10.1007/978-3-030-98785-5_11.

[15] X. Fan, J. Heidemann, and R. Govindan, "Identifying and characterizing anycast in the domain name system," USC/Inf. Sci. Inst., Marina Del Rey, CA, USA, Tech. Rep. ISI-TR-2011-671.

[16] X. Lee, Z. Yan, and R. Chaparadza, "Scaling the number of DNS root servers with internet," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2014, pp. 248–253.

[17] C. Li, Y. Cheng, H. Men, Z. Zhang, and N. Li, "Performance analysis of root anycast nodes based on active measurement," *Electronics*, vol. 11, no. 8, p. 1194, Apr. 2022, doi: 10.3390/electronics11081194.

[18] RIPE. (2023). *What is RIPE Atlas?* Accessed: Apr. 1, 2023. [Online]. Available: https://atlas.ripe.net/about/

[19] (2023). *BGPSTREAM*. Accessed: Apr. 1, 2023. [Online]. Available: https://bgpstream.caida.org/

[20] J. Abley, "Hierarchical anycast for global service distribution," ISC Tech. Note 2003-1, 2003.

[21] T. Koch, E. Katz-Bassett, J. Heidemann, M. Calder, C. Ardi, and K. Li, "Anycast in context: A tale of two systems," in *Proc. ACM SIGCOMM Conf.*, Aug. 2021, pp. 398–417.

[22] R. Austein, *DNS Name Server Identifier (NSID) Option*, document RFC 5001, Aug. 2007. [Online]. Available: https://www.rfc-editor.org/info/rfc5001, doi: 10.17487/RFC5001.

[23] N. Brownlee and E. Nemeth, "DNS root/gTLD performance measurement," in *Proc. Passive Act. Meas. Workshop*, 2002.

[24] A. Flavel et al., "FastRoute: A scalable load-aware anycast routing architecture for modern CDNs," Tech. Rep., 2015.

[25] Init7 NoC. *BGP Communities for Init7 Customers*. [Online]. Available: https://as13030.net/static/pdf/as13030_bgp_communities.pdf

[26] R. Schmidt, J. Heidemann, and J. H. Kuipers, "Anycast latency: How many sites are enough?" Inf. Sci. Inst., Univ. Southern California, Los Angeles, CA, USA, Tech. Rep., 2017.
[27] Y. Hyun et al., "Traceroute and BGP AS path incongruities," Tech. Rep., 2003.
[28] J. Pang, J. Hendricks, A. Akella, R. De Prisco, B. Maggs, and S. Seshan, "Availability, usage, and deployment characteristics of the domain name system," in *Proc. 4th ACM SIGCOMM Conf. Internet Meas.*, Sicily, Italy, Oct. 2004.
[29] A. Ramdas and R. Muthukrishnan, "A survey on DNS security issues and mitigation techniques," in *Proc. Int. Conf. Intell. Comput. Control Syst. (ICCS)*, Madurai, India, May 2019, pp. 781–784, doi: 10.1109/ICCS45141.2019.9065354.
[30] J. H. Kuipers, "Analyzing the K-root DNS anycast infrastructure," Tech. Rep., 2015.

ZIJUN LI received the bachelor's degree from the School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, China. She is currently pursuing the master's degree in engineering with the Harbin Institute of Technology, Harbin, China. Her research interest includes cyberspace security.

CHAO LI received the M.E. degree from the School of Computer Science and Technology, Southwest University, Chongqing, China, in 2015. He is currently pursuing the Eng.D. degree with the Harbin Institute of Technology, Harbin, China. His research interest includes cyberspace security.

GUOYING SUN received the M.E. degree from the School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, China, in 2015. He is currently pursuing the Eng.D. degree with the Harbin Institute of Technology, Harbin, China. His research interest includes cyberspace security.

ZHAOXIN ZHANG received the Ph.D. degree from the School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China, in 2007. He is currently a Professor with the Faculty of Computing, Harbin Institute of Technology. Besides, he is the Research Director of the Network and Information Security Technology Research Center, Harbin Institute of Technology, Weihai. His research interests include network and information security, network simulation, and domain name system security.

YANAN CHENG received the Ph.D. degree from the Harbin Institute of Technology, Harbin, China, in 2023. He is currently a Lecturer with the Faculty of Computing, Harbin Institute of Technology. His research interests include network and information security and domain name system security.

MUXIN WENG is currently pursuing the B.E. degree with the Harbin Institute of Technology, Weihai, China. His research interests include cyberspace security and embedded systems.