Tuning Fine-Grained Censorship: Assessing the Impact of Path Diversity on the Effectiveness of Internet Censorship

Abstract

Internet censor is typically deployed by authorities to serve the purpose of restricting people from accessing the Internet. In most cases, censorship deployment is following nationwide policies. However, the deployment and implementation of censorship may be highly diverse at the ISP level. Due to the limitation of measurement methodology, empirical studies mainly focus on country-level characterization. Therefore, we attempt to explore and analyze fine-grained censorship by identifying the diverse censorship deployment in one country. By leveraging end-to-end measurement approaches, we can explore multiple paths from one single vantage point. specifically, we deploy back-end servers distributed worldwide as the destination IP. The packets which carried the same test domain but with a different destination IP will be forced to traverse different border networks. By means of this, the requests will be examined by different censors if present. Our work aims to conduct end-to-end measurements to explore various paths on a global scale. Through a 5-month-long experiment with 19,642,104 requests sent by 47,558 unique IP addresses, belonging to 154 countries. we find India, Bangladesh, Vietnam, France, Venezuela, Nepal, Algeria, Taiwan, Serbia, and Bahrain are the top 10 countries with path diversity of censorship activities. Also, we find this issue is prevalent across 99 countries that have been found path diversity over 105 countries have censorship detected. we present extensive case studies to illustrate the configurations that lead to path diversity and explore the causes.

1 Introduction

1. Internet censors have been deployed by many governments and authorities to restrict users from accessing specific Internet services. Although many censor techniques, such as ??? [], have been proposed to achieve superior access control, the placement of Internet censors is consistent: they are placed on the network path between the users and the Internet services. Ideally, to achieve excellent censorship, the government and authorities need to ensure that every request must be inspected by at least one Internet censor before reaching their destinations.

2. Unfortunately, such a requirement poses a realistic challenge to the deployment of Internet censors. In the network, it is prevalent that each user request is routed differently due to potential network congestion, load balancing, or change of routing tables. Hence, the network paths taken by the requests could be inconsistent and unpredictable. On the one hand, if censors are not present on some network paths, users could access any service on the Internet without restrictions or supervision. On the other hand, if the censors on different network paths are not identical, user requests could be examined under different regulations. This can also lead to users accessing prohibited Internet services.

While many previous studies have focused on ??? [], little research investigates the deployment of Internet censors on different network paths. one of the closest studies is [] which studies the decentralized censorship control in Russia, but it relies on activists on the ground to obtain multiple leaked block lists. Another close work is [] studied the changes of DNS censorship detection when changing the packet fields

4. Our paper bridge the gap of ???. In this work, we design and implement *Pathfinder* to explore the impact of path diversity on HTTP censorship. We leverage the design of Disguiser and prior work to develop our own methodology and associate tools. We utilize Proxyrack, a residential SOCKS proxy to gain access to hundreds of vantage points remotely. Moreover, we set up 6 control servers distributed around the globe by Amazon AWS. By modifying the destination IP in the HTTP header field, we change packet parameters to prompt the HTTP request to different paths, reach our control server, and obtain responses for particular domains. The domain list was an empirical list leveraged from the prior work.

5. With *pathfinder*, we conducted 20 weeks of experiment and our vantage points were distributed in 154 countries. We have monitored the censorship activities in 154 countries. A key insight is that we find ??% path diversity in total censorship detected. This path diversity has induced censorship variation from vantage points. More important, we investigated

deeper into how prevalent this phenomenon is and which country suffers the most from this issue. In particular, we also find a security risk because some path has a lower percentage of censorship than other paths. This will result in censorship evasion on particular servers which host sensitive domains prohibited by censorship policy. In our study, we evaluate the impact of path diversity on censorship via different domains. According to our data analysis, We proved that censorship distribution is symmetric across domains.

6. We also investigate further in three countries, India, China, and Korea. From India, we monitored a path toward the Middle East that has less censorship than other paths. This issue creates a high risk of evading the censorship scan and illegal access to prohibited content online. In China's case, we find the availability of access to the domains that suppose to be blocked by the censorship policy. Besides, we also find a blockpage within the censorship techniques of China. In Korea's case, we explore that one prohibited domain was hosted by a parking server that cause no censorship in a particular path.

The remainder of this paper is structured as follows. Section 2 . Section **??** . Sections **??** presents . Section 6 uncovers. Section 7 discusses limitations and future work. Section 8 surveys related work, and finally Section 9 concludes our paper.

2 Background

Censorship Techniques. Internet censors operate on the application level of the network to detect and block illegal traffic. primarily use domain blocklist?. (censors also can block ips which is at ip-level. In addition, they can block urls or maybe some keywords.) In general, censorship can be categorized into two main groups based on the type of network traffic monitored, including DNS censors [] and HTTP domain censors [](given that censors can block domains, ips, and beyond, this categorization may not be appropriate). Specifically, DNS censors inspect all DNS traffic to identify domain resolution queries for unauthorized domains. If such queries are detected, DNS censors can either intercept the connection by dropping the DNS queries or manipulate the DNS responses to provide incorrect IP addresses. Similarly, HTTP domain censors inspect all HTTP traffic that passes through their hosting nodes. Such censors can monitor two domain requests to distinguish illegitimate communications: (1) IP addresses and (2) domain names. Unlike pure IP-address based censors which can cause significant collateral damages [], domain-name based censors can accurate domain blocking. Because of this, most Internet censors are domain-name based censors [] (I haven't seen such a conclusion in previous studies, could you share the reference?).

Similar to the man-in-the-middle (MITM) concept, domain-name based HTTP censors are deployed in the ISPs between users and domain servers to inspect all HTTP traffic []. In Figure 1, we illustrate four scenarios that could occur on the HTTP request routing path. In scenario ❶ where a user visits a legitimate domain server, the Internet censor only observes the communication without taking any actions. However, if the censor detects that the user attempts to establish a connection with an illegitimate domain, it can take three different actions to sabotage the connection depending on the censor's configuration. Scenario ❷ illustrates the censors tearing down the connection by sending RST/FIN packets to both the user and the hosting server of the illegitimate domain. In scenario ❸, the censor responds to the user with a block page. Usually, a block page serves the purpose of informing the user that the connection is terminated by censors due to the domain blocking policy. In addition to both scenarios, an Internet censor can simply drop all packets sent to the illegitimate domain (shown as scenario ❹ in Figure **??**). This causes an HTTP timeout on the user's side, which prevents the user from visiting the domain host.

There are two possible locations for censors to appear in a network connection. On the one hand, a censor can be located near the user's side to prevent traffic from reaching out to illegitimate domains. Such a censor is considered an outbound censor. Outbound censors are commonly seen at the country level, where governments block part of the Internet services due to potential race, political, and religion reasons. On the other hand, inbound censors appear near the domain server to deny packets from reaching the inside of the network. These censors serve similar purposes as a firewall so that services within the network cannot be accessed by unauthorized visitors. give two previous study about inbound censors, such as [8].

On-path and In-path Censors. In order to examine network traffic, censorship devices can be deployed in two different ways. An on-path censor is a device attached to a router that can obtain a copy of all the packets passing through the router. Since it cannot operate on the original packets, it is unable to prevent the packets from reaching their destinations. Correspondingly, it needs to inject packets to interfere with or terminate a connection.

An in-path censor acts as a Man-In-The-Middle (MITM) to examine the actual packets. Therefore, it can directly manipulate or drop the packets associated with the prohibited services. The in-path device is usually hard to be identified; however, due to the capacity of operating on the actual packets, it can be efficiently detected in our end-to-end framework.

Inbound and Outbound Censorship.

3 Pathfinder

In this section, we present an overview of the path diversity issue in censorship. We also introduce a systematic measure-

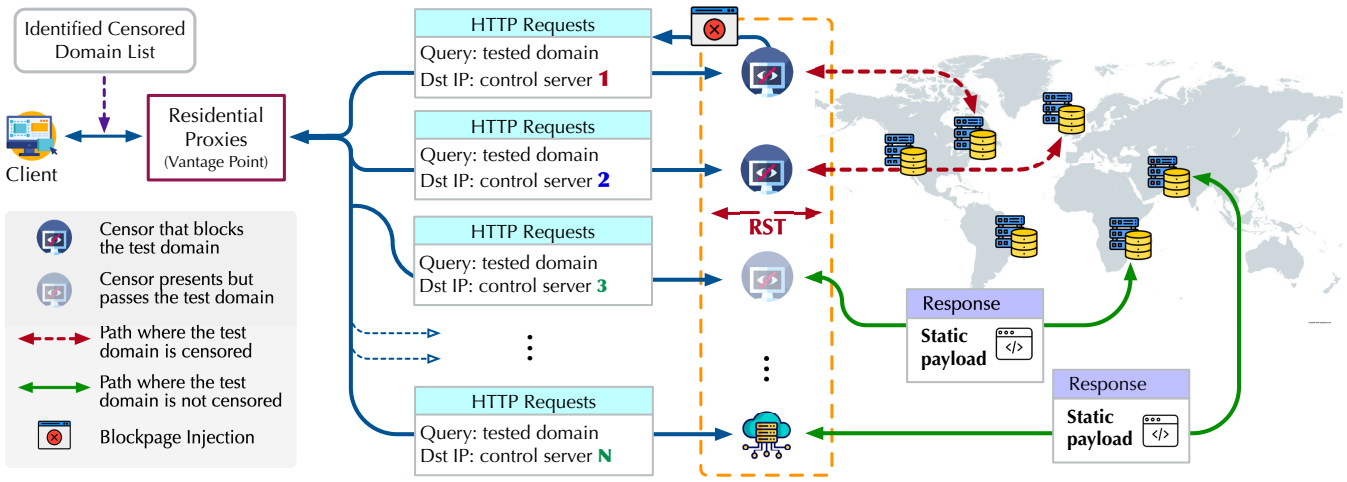

Figure 1: Overview of path diversity on Internet censorship and system design of *Pathfinder*

ment framework named *Pathfinder* to discover the censor deployment issue for different (routing path?). In addition, we discuss our methodology to mitigate all ethical concerns raised by our measurements.

3.1 Motivation

what is path diversity, why we need to measure path diversity, what security risk can caused by path diversity

For many reasons such as traffic load balancing [] (or change of the routing table? []), each HTTP connection between a user and a domain server may be routed to a different path. Ideally, Internet censors should be deployed in a way that all network traffic should be inspected by at least one censor before they leave the regional(local?) network. However, our study uncovers that for some routing paths, HTTP traffic could escape censorship inspection. To the best of our knowledge, we are the first to conduct a systematic measurement of the HTTP censorship deployment issue caused by path diversity.

Figure 1 demonstrates an overview of path diversity in Internet censorship. A vantage point attempts to establish HTTP connections to many domains hosted by different servers, and each connection may be routed to a distinct path. Normally, if the queried domains are uncensored, the vantage point should be able to access these domains without interference from any censors in the path. On the other hand, if the vantage point attempts to communicate with censored domains, such network traffic should be detected and blocked by any censors deployed in the middle of the communication channels. If the censors are not universally deployed in all paths, we can observe that some communication channels are intercepted by some sensors (shown as red dotted arrows in Figure 1), while other channels do not experience connection blocking (shown as green arrows in Figure 1).

The issue of path diversity in Internet censorship poses a realistic security vulnerability?. Taking advantage of such an issue, users can circumvent censorship simply by investigating censor behavior for all possible paths. Users can utilize network paths that are not fully covered by Internet censors to gain access to censored domains without being detected. Such a vulnerability can be exploited by any users given that they are able to discover the lack of censorship activity on some network paths. This is the primary motivation for this study. In our study, we aim to comprehensively understand the vulnerability of path diversity in Internet censorship.

3.2 Pathfinder System Design

how we design pathfinder

Inspired by previous studies [**?**, **?**], we develop *Pathfinder* to perform end-to-end measurements on censor behavior in different paths. Figure 1 presents the system architecture of *Pathfinder*. Specifically, *Pathfinder* involves communication between two major parties, *i.e.*vantage points, and control servers. On the one hand, a client commands vantage points to (1) construct HTTP requests with our test domains, (2) send the requests to our control server, and (3) collect responses for result analysis. Sending our constructed HTTP requests to control servers can trigger Internet censors along the path, if the test domains are to be blocked. By analyzing the response received from the vantage points, we can determine if there is an Internet censor in the communication paths. On the other hand, control servers respond to all inbound HTTP requests with a static payload. Such a payload indicates that HTTP requests have reached the control server without any interference from any Internet censors. An advantage of *Pathfinder* is that the censor activities can be fine-grained to each communication path. We can observe the response from vantage points to identify censorship with high accuracy.

Vantage Points. Vantage points serve the purpose of TCP proxies. Using these vantage points, we are able to send HTTP domain requests from IP addresses across the globe. Internet censors cannot differentiate our proxied requests from normal network packets. Therefore, such requests can realistically simulate the network traffic generated by a user who attempts to visit our control server using HTTP requests. By successfully receiving a valid response from the targeted domain, we prove that no Internet censors take any action to interrupt our communication. Otherwise, we can confirm that an Internet censor is placed along the path between the user and the domain hosting server.

Domain List. We leverage the list of domains used in the previous study [12], which included a set of popular domains and sensitive domains. The popular domains are extracted from Alexa's top 1,000 domains [1], while the Citizen Lab [7] consists of a global test list and a country-specific test list. We filter the Citizen Lab list by country and insert popular domains from Alexa's list and the global test list. As such, we have a compiled list sorted by country that has potential censored domains. limitation: previous paper does not consider different path, so the domain list from previous paper could be limited.

HTTP Domain Requests. We utilize each vantage point as a proxy to send HTTP requests to our control servers. The HTTP request is carefully constructed. Every request is carefully constructed so that the *HOST* header contains a domain name from our domain list and the destination is set to one of the IP addresses of our control servers. Also, we configure the request to have a relatively short timeout (*e.g.*5 seconds) so that we do not need to wait an extended period of time if an Internet censor drops our requests. In addition, *Pathfinder* automatically retries the timeout requests four more times before declaring it to be blocked by the Internet censors. This reduces the chance that our domain requests are dropped due to network traffic congestion.

Control Server. Control servers play a key role in establishing path diversity for different HTTP requests. Because each control server is hosted at different locations, HTTP requests must be routed differently to reach their destinations. Unfortunately, we cannot obtain the exact path of each HTTP request due to the lack of application Traceroute capability in the vantage points. Control servers provide a static payload for every HTTP request received. The content of the static payload is unique in a way that it must not collide with other legitimate domain pages or blockpages.

3.3 Special Design Consideration

Eliminating Cache Proxies. We also consider a special case when there is a cache proxy in the middle of the path to intercept our packets. However, instead of querying our control server, the packet is re-routed to the actual domain server. In this situation, the vantage point may receive the actual domain page instead of our static payload. Such path should be considered as no censorship, however, we have not found any existing tools to validate that the received domain page is legitimate. Also, developing such a tool is out of our research scope. Hence, we perform a cache proxy test for every vantage points, and if a cache proxy is detect, we automatically discard the vantage points.

Based on the previous study, the cache was utilized to reduce network traffic and latency. Empirically, it will simply happen in local browsers or ISPs to preserve a landing page of a website that has been frequently visited by users. Thus, the cache proxy may intercept the measurements by sending preserved contents back to the client side. It interferes with the observations for censorship since HTTP requests neither arrive at the destination server nor trigger the censors in the path. Also, the cache proxy will return a response that creates harassment and generate false positives.

In this experiment, we need to investigate each vantage point we obtain from Proxyrack and make sure there have no cache proxies in the middle. Therefore, we filter those cache-inserted vantage points out of our testing lists before we initiate our tests. The following table is about the number of caches detected in around 1 day (from Jul20 14:00 pm to Jul21 16:00 pm). The total of caches observed from the experiment is 885. This data shows that vantage points with cache consume nearly 1/3 of the total vantage points acquired. Thus, it is definitely significant to conduct a cache test before issuing requests to the control servers. Since the static payload of the reference server is unique and different from the static payload crafted for identifying normal HTTP responses. Thus, the data archived from the reference server is also considered as ground truth for Cache Detection Test. In sum, it is necessary to eliminate the impact of invisible cache before launching experiments in order to reduce false positives.

Before we add the Cache Test to our experiments, we observed suspicious vantage points mostly taking a large amount of the total vantage points we archived in a tested cycle(7 days). For instance, per every 10 vantage points responses received from the control server, up to 7/8 vantage points we could monitor distinguished HTTP responses such as static payload vs. censor behavior in countries like South Korea and Japan. However, after we add the Cache Test, the number of countries we acquired vantage points from is increasing. But the number of suspicious vantage points we observed is decreasing sharply among those countries we observed. We eliminate cache-poisoned vantage points, once we found one of the paths got inserted cache, we extract this vantage point to evade the impact of rerouting by the cache.

Eliminating Inbound Censors. As mentioned in Section **??**, Internet censors can appear as inbound censors and outbound censors. Our (disguisor) tool can effectively identify Internet censor between vantage points and our control servers, but it cannot distinguish the location in which censors appear in a path. Therefore, we conduct additional experiments to eliminate the effect of inbound censorships in our study.

In addition, we conduct further experiment to verify that there is no inbound censorship in our control servers. This experiment has two steps. First, we set up multiple reference servers on Amazon AWS that are hosted in many countries. These servers act similar to one of our Vantage Points. Then, send HTTP requests with the test domain list that suppose to trigger In-bound censorship if it existed on the control server side. We confirm that no censorship appears between our control servers and our reference servers.

Next, we establish additional reference servers using VPN services (hidemyip). We randomly select 5 VPN servers from each continent and we execute traceroute to each control server using the disguisor. We exclude domains that are previously identified as censored domains. We confirm that all queries have successfully returned with a static http package, meaning that no censorship is detected in the control server side.

4 Experiment

4.1 Experiment Overview

Our study lasts 20 weeks from May 11, 2022 to September 28, 2022. We take advantage of the residential proxy network provided by Proxyrack [] as our vantage points. For control servers, we initiate 6 EC2 instances in different regions of Amazon AWS [].

4.1.1 Vantage Points.

Proxyrack enables us to test censorship on a large scale both quantitatively and geographically. It attracts a large number of participants to share their residential IP addresses as proxy nodes in exchange for financial profits []. These participants are located around the world. This significantly benefits our measurement, allowing us to investigate Internet censorship using a large number of proxy nodes in many different countries. However, we find that proxy nodes in some countries have a higher chance of being offered to users by Proxyrack. For example, we observe many proxies located in South Korea, Japan, and Brazil, but not in countries such as Cuba, Myanmar, and Bolivia. To further balance the number of proxies we obtain from Proxyrack, we configure *Pathfinder* to only test 80 vantage points per country per week. This increases the opportunity for us to obtain vantage points from countries with a lower chance of being selected by Proxyrack.

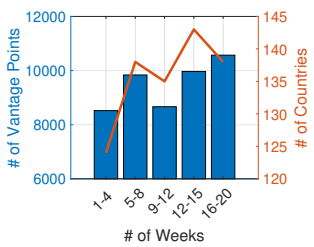

Figure 2: Vantage points explored for each week, as well as their country coverage.

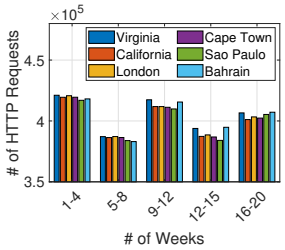

Figure 3: Number of HTTP request received by each control servers.

In total, during the 20 weeks of our experiment, we explore 46,150 vantage points located in 154 countries. Figure 2 shows the distribution of the number of selected vantage points, as well as the number of countries covered each week.

4.1.2 Control Servers.

We carefully select our control servers using two criteria: (1) control servers must be widely spread across the world, and (2) there should be less censor activities in the hosting countries. Following both requirements, we establish six servers on Amazon AWS, each of which is hosted in a different region. The blue rounded points in Figure **??** illustrate the locations of our selected control servers. Specifically, these servers are located in Virginia (North America), California (North America), Sao Paulo (South America), London (Europe), Bahrain (Middle East), and Cape Town (Africa).

During our 20-week experiment, all six control servers receive 12,068,544 HTTP requests sent from vantage points. Figure 3 presents the number of HTTP requests received for each control server.

4.2 Ethical Consideration.

Our experiment is carefully designed to minimize the ethical concerns raised by large-scale censorship studies. Measuring censor activity using *Pathfinder* does not involve human participation, nor do we collect sensitive information about any person or entity. Therefore, our study is exempted by the institutional Internal Review Board (IRB).

Furthermore, we rely on Proxyrack to provide a large number of residential proxy nodes for our censorship measurement. Such a service has been used by many previous censorship studies, such as []. We pay the subscription fees to Proxyrack, which cost USD120 per month. We gain access to the Proxyrack service through its official software APIs. In addition, we avoid using the same residential proxy repeatedly, so that our experiment poses little risk to the owners of the proxies.

Furthermore, our experiment is conducted solely between the residential proxies obtained from Proxyrack and our control servers hosted on Amazon AWS. No communication is

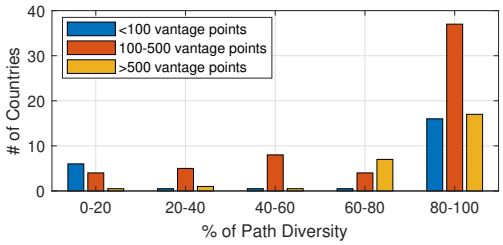

Figure 4: distribution of path diversity percentage for different countries.

established with the real censored domains, which protects the owner of the residential proxies from any potential security risks. We provide a detailed explanation of our experiment in the static payload of our control server along with our contact information. During the entire period of our experiment, we have not received any concerns regarding our methodology and data collection.

5 Result & Analysis

We conduct a large-scale measurement on the path diversity of Internet censorship using *Pathfinder*. In this section, we present ourresults in detail. We also analyze our results.

5.1 Results

Within the 154 countries, we observe ??? countries with censor activities, accounting for ??% In these countries, no HTTP requests are blocked by censors. This data aligns with the previous studies. [] demonstrate that these countries have less censorship. Also, ??? countries have only record ??? vantage points. The less vantage point in these countries could results in our experiment missing censors in these countries.

The rest ??? countries, we record at least 1 vantage points with censorship. Figure ??? shows the censorship diversity for countries with less than 100 vantage points within these countries, ??? countries record less than 100 vantage points. While it is uncertain how censorships behave in these countries in general due to the lack of vantage points, we did found ??? countries with path diversity issues. Particularly, countries such as ???, ???, are collected ??? vantage points, but all of them experience path diversity issue, which account for ???%. This number means that users in these countries may easily circumvent censorships.

between vantage points from 100 to 500, we record ??? countries. Figure ??? shows the censorship diversity for countries between 100-500 vantage points.

25 countries with more than 500 vantage points, together, they account for 74.4% of the total vantage points. Figure ??? shows the censorship diversity for countries with less than 100 vantage points table 1 shows the censorship and diversity

Country	Vantage Point			Path Diversity Percentage
	Total	Censored	Diversity	
Brazil	907	7	7	100.00%
Poland	647	3	3	100.00%
India	637	373	373	100.00%
Sweden	599	11	11	100.00%
Spain	550	17	17	100.00%
Argentina	541	29	29	100.00%
Ghana	518	6	6	100.00%
China	506	478	478	100.00%
Australia	502	97	95	97.94%
Indonesia	579	215	207	96.28%
Japan	1,183	323	306	94.74%
Chile	503	19	18	94.74%
Taiwan	624	36	32	88.89%
Singapore	501	89	79	88.76%
Bulgaria	603	7	6	85.71%
Latvia	529	19	16	84.21%
Hong Kong	762	41	33	80.49%
Vietnam	612	433	328	75.75%
Russia	699	529	400	75.61%
United States	689	84	61	72.62%
Italy	575	24	17	70.83%
Canada	677	64	45	70.31%
Ukraine	617	108	71	65.74%
Thailand	566	207	129	62.32%
South Korea	1,245	617	238	38.57%
Total	35,503	7,115	5,619	78.97%

Table 1: List of countries/regions with more than 500 vantage points and their path diversity percentage.

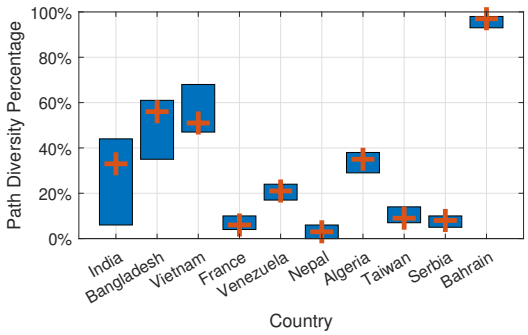

Figure 5: Top 10 countries with path diversity of the censorship.

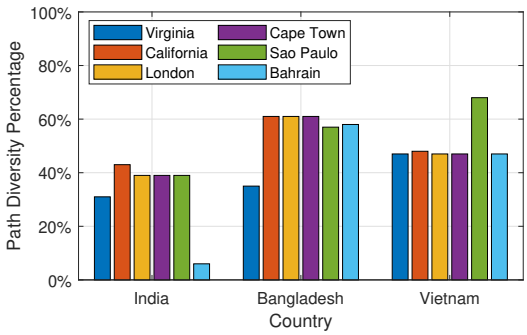

Figure 6: distribution of censorship path diversity.

details about these countries. From the table, we can observe 8 countries with 100% path diversity, representing 32% of the total countries.

After we investigated the data sets, we categorize three types of measurement results pinpointing the path diversity. One is no censorship for all paths, the other is all paths blocked by censors, and last is some paths been blocked but still have accessible paths, namely "some-have-some-not". Table 1 shows censorship diversity in the percentage of the total censorship behaviors sorted by country. We find that 33 countries have path diversity in total censorship behaviors, they are listed in Table 1. As proof, this phenomenon is prevalent across a large portion of test countries. In particular, at least one path circumvents the censor system causing path diversity. Other 11 countries, such as Kuwait, Australia, Portugal, and Indonesia...also presents a high percentage showing the path diversity happens at almost every detected censorship. We filtered the dataset in 200 thresholds in each country, since our experiments last 20 weeks and we focused on the countries that collected an average of 10 vantage points each week. From the counties that exceed 90% percentage of path diversity consuming the total censorship behaviors, we find most of the countries are located in Europe. Either we observed a small fraction of this path diversity affecting the censor behaviors in 22 countries, which percentage in Table1 lower than the percentage of 40%. We observed the opposite bell shape of the percentage distribution in Table1. The number of countries in the middle, which has a percentage of 50% - 89% is far less than the other two categories. In sum, we observe the prevalence of censorship diversity via the path by the percentage that takes up the total censorship activities which are listed in Table 1. Also, we find the censorship normalized distribution on each path for other countries that have no path diversity.

what happen to countries with less than 200 vantage points.

The purpose of this study was to investigate the path diversity in each potential path toward different servers to reveal censorship changes. In Figure 4, we show the top 10 countries with path diversity of censorship activities. This lower bound is the lower percentage we detected censorship on one of the paths. The upper bound is the highest percentage of censorship we detected on particular paths. We have 6 paths in total. Moreover, we labeled the mean of the percentage of censorship behaviors among the paths. From Figure 4, we find India, Bangladesh, and Vietnam have outstanding differences between the upper bound and lower bound. Besides, other countries have small differences between the upper bound and lower bound. For the other countries not in the top 10, their censorship behaviors are evenly distributed by paths. We did not find any path that has an exceptionally high or low percentage of censorship activities. This also verifies our findings are synchronized with the previous studies and common knowledge on censorship deployment's continuity and consistency.

also, the path diversity for each country is different.

In Figure 5, we elaborate on the path diversity in India, Bangladesh, and Vietnam because the path diversity in these 3 countries has drawn our attention. In India, the path from India to Bahrain(Middle East) has detected far less censorship than the other paths. In other paths based on our experiment set-up, we observed the percentage of censorship on each path ranging from 18.74% to 26.50%. Thus, the path toward Bahrain(Middle East) shows a pretty low percentage than the other paths, which means it is easy to bypass the scanning of the censors in the middle of the path.

In Bangladesh, the path from Bangladesh to Virginia(the East coast of the U.S.) has detected far less censorship than the other paths. In other paths based on our experiment set-up, we observed the percentage of censorship on each path ranging from 47.61% to 50.70%. Thus, the path toward Virginia(the East coast of the U.S.) shows a pretty low percentage than the other paths, which means it is easy to bypass the scanning of the censors in the middle of the path.

However, the case in Vietnam is different. In Vietnam, the path from Vietnam to Sao Paulo(South America) has detected a large percentage of censorship than the other paths. In other paths based on our experiment set-up, we observed the percentage of censorship on each path ranging from 32.92% to 33.87%. Thus, the path toward Sao Paulo(South America)

shows a high percentage than the other paths, which means it is easy to hit the censors in the middle of the path.

5.2 Analysis

To this end, we analyze the collected data sets to answer a series of research questions on the influence of path diversity on the effectiveness of Internet censorship:

5.2.1 In general, how prevalent of path diversity in censorship behaviors across countries?

We will utilize the proposed framework in Figure 6 to conduct large-scale, longitudinal measurements to understand the presence of this phenomenon and quantify its prevalence in each country that has been observed with censorship activities. Typically, censorship has been adopted by a large number of countries through networking to restrict people's access to the Internet. Since the previous studies focus on measuring the censorship behaviors, techniques, and deployment, most of the time there only utilized one control server. Then they investigated the path between various vantage points toward a fixed server. Therefore, a few previous studies recognize this issue even though they monitor changes in censorship behavior. They may still consider it was some interference in the network traffic. However, according to our measurements, we identify that path diversity has a certain impact on censorship behaviors among half of the countries in the world. Based on our observation, there are 105 countries that have detected censorship. We find 99 of them that have path diversity and detected *some-have-some-not* censorship behavior. Namely, this path diversity happened in the majority of countries that are under censorship policies. Thus, we can conclude path diversity is a prevalent phenomenon affecting censorship activities worldwide. Also, we find suspicious vantage points in several countries where we observe censorship changes by modifying path parameters. In specific, this phenomenon is more likely to happen in countries with heavy censorship.

5.2.2 How extensively does path diversity affect censorship in countries that enforce strict censorship policies?

Through detailed case studies, we will then focus on the censorship variation caused by path diversity in those countries that have observed severe Internet censorship. In addition to the censorship detection using probing packets, we will also leverage VPN vantage points to perform both application and network-layer trace routes unveiling specific configurations and deployments that cause such diversity.

In our dataset, we observed *some-have-some-not* resulting in censorship variation mostly happening in countries with heavy censorship policies. We note that path diversity is a prevalent phenomenon across countries. Further, we examined our data sets to explore the relationship between path diversity and the extent of censorship activities. Empirically, the censorship changes clarified as *all-or-nothing*, meaning that either we observed no censorship or "expected" censorship activities. [4] In HTTP protocol, "expected" censorship is the interception implemented by inserting a block page, RST/FIN packet injection, and packet tear-down. Here, we investigated censorship outcomes in each path taken by HTTP requests synchronize with test domain lists to various control servers. For each country, we focus on the total of censorship activities and censorship variation caused by path diversity. We verify our experiment by comparing the censorship percentage with the empirical studies. As such, we find the censorship notorious countries China, Pakistan, India, Kuwait, Vietnam, Russia, and Bangladesh show a high percentage of censorship across total vantage points collected. We either observed a high percentage of *some-have-some-not* in those countries. In our raw data, the total number of vantage points collected for referenced countries is over 400. The percentage of path diversity in total censorship is 74.93% - 100%. As proof, path diversity excessively impacts countries with heavy censorship policies. Another key finding of censorship deployment shows normalized distribution on each path in most countries. We examined the percentage of censorship activities on each path sorted by country. The observation is most of the censorship activities are deployed uniformly on each path toward the servers over the world.

the more censor total, the more suspicious VPs. Figure

5.2.3 Can specific paths that experience less censorship be leveraged to achieve detour for censorship circumvention?

Based on the observations made from our large-scale measurements, we will leverage CDN's distributed infrastructure to explore a censorship-aware mapping system that could achieve a detour for rerouting the packets to a different path to circumvent certain censorship.

It may cause potential risk to the censorship deployment because the percentage of a particular path is exceptionally low when compared with other paths. For instance, we monitored the path from Finland to the control server in Bahrain(Middle East) has no censorship. Although in other paths from Finland to Bahrain, we observed censorship on some of the vantage points takes up to 16.67% - 33.33% of the total. Thus, if someone intentionally constructed a server in Bahrain and used it to host several prohibited websites against the law of Finland, the citizens over there still have a chance to access those contents online because of this glitch. This will create a potential risk either in censorship deployment or from the ethical point of view. On the opposite, we observed some path

has a comparatively high fraction of censorship than other paths in specific countries, meaning that if we detour to the other paths we will have less chance to hit the censors. To illustrate, we collected 34,522 vantage points in Vietnam and 23,316 of those have detected censorship activities on the path from Vietnam to Sao Paulo while other paths have observed a lower percentage of censorship activities. If the clients in Vietnam happen to visit the domains hosted by the servers in countries other than Sao Paulo, it has less chance to encounter the censors. This phenomenon also appears in Georgia. We collected 40 vantage points in Georgia while 20 of them have outstanding censor behaviors on the path to California, North America. However, we find less censorship on the other paths that are far less than the one to California. That means if we skip that path we will probably not encounter the censors.

5.2.4 Do other factors affect the occurrence of censorship diversity?

In addition, we will design extensive experiments to investigate what factors may also influence censorship diversity. For example, the provider of servers... Also, even toward the same location, different destination networks may change the routing paths so as to the censorship experienced by the probing packets due to the highly diverse peering relationship. Thus, we will deploy multiple control servers at the same locations to test whether the changed destination networks would also affect censorship.

We evaluate the censorship extent on each path and find out some path shows a low percentage of censorship activities than other paths. Further, we explore the relationship between path diversity and domains. Because we aim to evaluate the impact of path diversity differs in various test domains. We assumed there has no difference on each path based on the censorship system is designed symmetrically. [10, 16] In particular, we leverage the test lists of domains from the prior work. [12] Based on our methodology, the test domain lists have been verified to have great possibilities to trigger the censors in the path. Pretend that, we take India as an example to illustrate the path diversity has little relevance to domains. In Figure.8, we present the distribution of censorship on each path across 10 domains. We find a similar distribution of censorship on each path to our control servers. On the path to Bahrain(middle east), censorship has shown a far less percentage than on the other paths. For other paths not shown in Figure.8, the distribution of censorship on each path is similar. Therefore, we proved the impact of path diversity on censorship behavior is consistent and continuity across domains.

To verify the factor of the cloud service provider, we carefully select the three most popular cloud services, AWS(Amazon), Azure(Microsoft), and GCP(Google Cloud Platform). For each cloud provider, we establish 4 control servers in Virginia(United States), Sydney(Australia), Paris(France), and Sao Paulo(South America). We replace the control server list of *Pathfinder* with the aforementioned 12 control servers that were set up on three cloud services. Also, we leverage the Proxyrack platform to acquire vantage points from ??? countries during a two-month-experiments. We issue HTTP requests through distributed vantage points with sensitive domain lists embedded to temper the censorship in the path toward control servers. Here, the providers of the control servers are different. One of the key findings is the censorship activities we observed from vantage points in South Korea pinpointing three control servers that belong to AWS. They are the control servers from Virginia (United States), London (United Kingdom), and Sao Paulo (South America). In other control servers, we received static payloads instead of censorship thus no censors in the path. Therefore, this phenomenon shows that even though the control servers are located in the same countries, different cloud services will detour the HTTP requests to a different path. As such, some HTTP requests will be blocked by the censors in the path, while other requests will successfully reach the destinated servers.

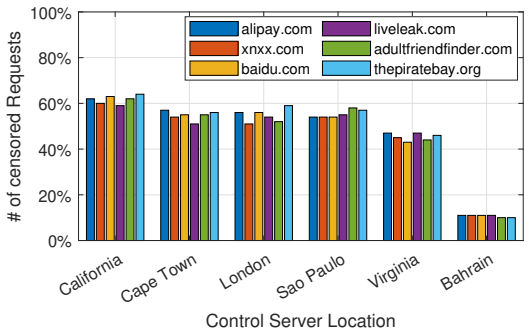

Figure 7: distribution of path diversity censorship percentage over the different domains.

Observation: From Japan's vantage point, we observed the censorship diversity in the experiment that has multiple servers in different regions. However, we have not seen censorship diversity happen in the experiment with servers that were located in the same geolocation but from different providers.

6 Case Studies

In this section ...

6.1 India

Section **??** demonstrate that vantage points located in India experience 100% path diversity. Also, from the control server point of view, path from India to Bahrain has lower censor activity than other control servers. Because of this, we further

conduct a case study in India, investigating in detail about the circumstances.

India has been identified as high censor activity in previous study. In our experiment, we use a blocklist for India, which contain ??? domains. we investigate a total of 637 vantage points provided by Proxyrack, and in total we send ??? http requests to control server.

We randomly select six domains from India's blocklist for further investigation. Figure 7 shows the percentage of censored HTTP requests for each control server. It is obvious that censorship to Bahrain has significantly low censor activity across all domains. While other paths have 40-60% of chance being censored, Bahrain only has 10%. This indicates that, in India, users could circumvent censorship using Bahrain server.

6.2 China

In this section, we elaborate on three case studies pinpointing three scenarios of censorship changes. For the first case study, we went through all responses from China. The tested domain lists are concatenated with the sensitive domains has been censored in the previous study. [12] Most of the censored techniques that block HTTP requests in China are xxx. We assumed there is no block page within the censored techniques utilized by the Great Fire Wall in China. Nevertheless, we observed several block pages on a particular domain by shuffling the destination IPs and obtained different censor behaviors in vantage points from China. one type of block page was issued by a local government that attempted to prohibit the citizens in a particular district to get access prohibited websites. This also created a diversity of censorship behaviors which not consistent with the China censorship mechanism. Other types of block pages were hosted by upstream servers and served as a gateway or proxy that intercepts the Internet traffic in China. The domains are https://mgbvp648.com and https://adsmg457.com. A key finding is these local servers are established before the national censorship thus resulting in different censorship behaviors. Moreover, because of the path diversity, we find the different censorship behaviors associated with different paths. Moreover, we investigate the duplicate vantage points we collected from China. We find that the same vantage point in which either the proxy information or the destination IP is the same has different censorship activities on the same domain. Surprisingly, we obtained the static payloads from the control server for Facebook.com and also monitored a blocking on the same vantage point on the other experiment attempts. These different censor behaviors on the same domain happened on one vantage point toward the same control server exactly showing the HTTP request took a different path that circumvent the censor's detection. As acknowledged, Facebook.com, Twitter.com, Google.com, Youtube.com, and Instagram.com, these domains were prohibited to access from China. However, we still observed the open access to these domains from China's vantage points which raised concerns about the packet paths diversity in censorship circumvention.

6.3 South Korea

South Korea is also known as a censor active country. Many domains have reportedly been blocked by South Korea government due to various reasons. Usually, when a user attempt to visit a blocklisted domain, censors intercept the requests and return a blockpage back to the user. This informs the users about any risks of visiting the site, and explain the regulations.

One domain that draw our attention is `onekorea.org`. In total, we send ??? domain requests to this domain, and ???% are blocked by censors. In particular, ??? of them receives government blockpage, ??? are timeout, and ??? are connection tear-down. As figure??? shows, ??? path experience less censor behaviors compare to others.

We dig deeper into the domain, and find that the domain is now a parking page hosted by GoDaddy. However, The fact that this domain receives government blockpage indicates that the domain is officially blocked by the government, meaning that the block should be country-wide. While the historical data of this domain is unknown to me, we suspect that the censor behavior change is due to the domain content change. For some path, the censors to this domain is released because the domain is now a parking page, and does not contain any unauthorized or malicious contents. However, such a censor release can only be observed in certain path. This further prove our observation that the censor deployment is not uniform for all path.

7 Discussion

does not know the exact path, vpn traceroute?

control servers cover as many paths as possible for larger test scales.

expand vantage point, specifically for countries that only have 1 vantage point, find more proxy or vpn services?

8 Related Work

8.1 Domain Censorship.

Some censorship measurements focus on particular countries, such as China [2,11], Iran [3,5], Syria [6], Pakistan [13], Kazakhstan [18], Russia [19], India [22]. Others focus on studying censorship in different scopes. [9, 14, 16–18, 20] These studies explore censorship in different protocols and conduct extended or concentrated measurements of censorship. Prior work has investigated China's border ASes network and relationship with foreign countries. [21] Some censorship measurements study what content will be blocked on the Internet. Others categorize censor techniques and discover the routes

of censor deployments. Prior research focuses on measuring a specific aspect of censorship, while most recent studies prefer to monitor censorship from a longitudinal point of view. As such, we may observe the censorship policy change over a long time scale.

Recent years have witnessed progress in implementing global censorship measurement on various platforms such as Censored Planet, OONI, and ICLab, as well as qualitative reports, such as the annual Freedom on the Net Report by Freedom House. Previous research dedicates to performing a wide coverage and longitudinal censorship measurement and utilizing remote measurement techniques to collect and analyze censorship data. Case studies on censorship events and analyzing trends in censorship methods and censored contents facilitate creating a comprehensive view of global censorship. [17] Since most of the investigated sites come from the Alexa top 10K most visited websites. Prior studies of censorship have been limited both in scale and in time, to obtain widespread, continuous measurements from a diversity of vantage points have proved difficult. The difficulty in recruiting vantage points across multiple countries, regions, and ISPs. [15]

However, none of these censorship measurements have explored the censorship variation due to the packet's *path* diversity resulting from the geolocations of destination servers.

8.2 Censorship Circumvention

add more paper here

Our paper differs from previous works in which we discover that censorship can be avoided by re-routing the domain requests to a different path. This significantly reduces the technical difficulties on the user's side. Any users who have knowledge on the path diversity of Internet censorship could run a test in their local network to figure out the path diversity. Form here, they could avoid censor.

9 Conclusion

In this paper, we present ... In the future, we aim to ... control servers cover as many paths as possible for larger test scales. expand vantage point, specifically for countries that only have 1 vantage point, find more proxy or vpn services?

References

[1] Alexa. https://www.alexa.com/topsites.

[2] Anonymous. The Collateral Damage of Internet Censorship by DNS Injection. *ACM SIGCOMM Computer Communication Review*, 2012.

[3] Simurgh Aryan, Homa Aryan, and J. Alex Halderman. Internet Censorship in Iran: A First Look. In *USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, 2013.

[4] Abhishek Bhaskar and Paul Pearce. Many roads lead to rome: How packet headers influence DNS censorship measurement. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 449–464, Boston, MA, August 2022. USENIX Association.

[5] Kevin Bock, Yair Fax, Kyle Reese, Jasraj Singh, and Dave Levin. Detecting and evading {Censorship-in-Depth}: A case study of {Iran's} protocol whitelister. In *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*, 2020.

[6] Abdelberi Chaabane, Terence Chen, Mathieu Cunche, Emiliano De Cristofaro, Arik Friedman, and Mohamed Ali Kaafar. Censorship in the Wild: Analyzing Internet Filtering in Syria. In *ACM Internet Measurement Conference (IMC)*, 2014.

[7] Citizen Lab. URL Testing Lists Intended for Discovering Website Censorship. https://github.com/citizenlab/test-lists/, 2019.

[8] Oliver Farnan, Alexander Darer, and Joss Wright. Poisoning the Well: Exploring the Great Firewall's Poisoned DNS Responses. In *ACM on Workshop on Privacy in the Electronic Society*, 2016.

[9] Arturo Filastò and Jacob Appelbaum. OONI: Open observatory of network interference. In *USENIX Workshop on Free and Open Communications the Internet (FOCI)*, 2012.

[10] Nguyen Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, and Michalis Polychronakis. How great is the great firewall? measuring china's {DNS} censorship. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3381–3398, 2021.

[11] Nguyen Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, and Michalis Polychronakis. How great is the great firewall? measuring china's DNS censorship. In *USENIX Security Symposium*, 2021.

[12] Lin Jin, Shuai Hao, Haining Wang, and Chase Cotton. Understanding the practices of global censorship through accurate, end-to-end measurements. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 5(3):1–25, 2021.

[13] Zubair Nabi. The Anatomy of Web Censorship in Pakistan. In *USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, 2013.

[14] Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, and Phillipa Gill. ICLab: A Global, Longitudinal Internet Censorship Measurement Platform. In *IEEE Symposium on Security and Privacy (S&P)*, 2020.

[15] Paul Pearce, Roya Ensafi, Frank Li, Nick Feamster, and Vern Paxson. Augur: Internet-Wide Detection of Connectivity Disruptions. In *IEEE Symposium on Security and Privacy (S&P)*, 2017.

[16] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. Global Measurement of DNS Manipulation. In *USENIX Security Symposium*, 2017.

[17] Ram Sundara Raman, Prerana Shenoy, Katharina Kohls, and Roya Ensaf. Censored Planet: An Internet-wide, Longitudinal Censorship Observatory. In *ACM Conference on Computer and Communications Security (CCS)*, 2020.

[18] Ram Sundara Raman, Adrian Stoll, Jakub Dalek, Armin Sarabi, Reethika Ramesh, Will Scott, and Roya Ensafi. Measuring the Deployment of Network Censorship Filters at Global Scale. In *Network and Distributed System Security Symposium (NDSS)*, 2020.

[19] Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi. Decentralized Control: A Case Study of Russia. In *Network and Distributed System Security Symposium (NDSS)*, 2020.

[20] Benjamin VanderSloot, Allison McDonald, Will Scott, J. Alex Halderman, and Roya Ensafi. Quack: Scalable Remote Measurement of Application-Layer Censorship. In *USENIX Security Symposium*, 2018.

[21] Xueyang Xu, Z. Morley Mao, and J. Alex Halderman. Internet Censorship in China: Where Does the Filtering Occur? In *Passive and Active Network Measurement (PAM)*, 2011.

[22] Tarun Kumar Yadav, Akshat Sinha, Devashish Gosain, Piyush Kumar Sharma, and Sambuddho Chakravarty. Where The Light Gets In: Analyzing Web Censorship Mechanisms in India. In *ACM Internet Measurement Conference (IMC)*, 2018.

APPENDIX

A An Example

Country	Percentage	# of Countries
Albania, Argentina, Belgium, Bosnia Herzegovina, Brazil, China, Czechia, Dominican Republic, Ecuador, Estonia, Finland, Georgia, Germany, Ghana, India, Kenya, Macao, Mexico, Moldova, Nepal, Nicaragua, Norway, Pakistan, Panama, Peru, Poland, Serbia, Slovenia, South Africa, Spain, Sweden, Uganda, Uruguay	100%	33
Kuwait, Australia, Portugal, Indonesia, Colombia, Israel, Chile, Japan, France, United Kingdom, Netherlands	90% - 99%	11
Taiwan, Singapore, Philippines, Bulgaria, Latvia, Venezuela, Hong Kong	80% - 89%	7
Vietnam, Russia, Greece, Bangladesh, New Zealand, United States, Italy, Canada	70% - 79%	8
Ukraine, Lithuania, Thailand	60% - 69%	3
Turkey, Kazakhstan, FrenchPolynesia, Belarus, Benin, Morocco	50% - 59%	6
SouthKorea, Iran, United Arab Emirates, Hungary	30% - 39%	4
Malaysia, Yemen	20% - 29%	2
Saudi Arabia	10% -19%	1
Armenia, Botswana, Cambodia, Costa Rica, Cyprus, Denmark, Guam, Iraq, Ireland, Malta, North Macedonia, Paraguay, Romania, Slovakia, Qatar	0% - 9%	15

Table 2: Fraction of VPs that Observe Censorship Diversity in Censored Countries > 200