# Differentiating Middle Box Blocking from Server Side Blocking

Anonymous Author(s)

**ACM Reference Format:**
Anonymous Author(s). 2019. Differentiating Middle Box Blocking from Server Side Blocking. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

## INTRODUCTION

## BACKGROUND

## 1 METHODOLOGY

We build on the technique proposed by Halderman (ref to the initial paper that proposed this). **discuss basic idea of the approach and add a summary of shortcomings of that approach; what practicalities does it ignore?**

### 1.1 Dealing with Multiple Paths

Because load-balancers can affect our measurements and conclusions, we fix the paths our probes take by initially keeping TOS, Protocol, Source Address and Destination Address fields of IP header constant for all the probes and then keeping certain fields of transport layer header constant in the following fashion (in line with the literature):

- For ICMP: ICMP Code and Checksum fields of ICMP echo header are kept constant for all ICMP probes sent towards one end-host.
- For UDP/DNS: Source port and Destination port fields are kept constant for each nameserver, as they are used to determine flow identifier for the probes. Destination port is fixed to port 53 for DNS service, whereas source port is randomly sampled from 20000-40000 range for each nameserver in the dataset.
- For TCP and HTTP: Just like DNS, only source and destination ports are the determinants for flow identifiers for TCP. Our destination port is fixed to 80, for probing the webservers. The value for source port is randomly sampled from 20000-40000 range, which is kept consistent for all probes targeted towards a particular webserver. This makes sure for a particular webserver our port numbers stay same and hence the flow of probes remain consistent. As HTTP probes are built on our TCP probes, the same argument hold true for them.

**Do our probes across different protocols take wildly different paths? We need some validation on this, and may need a strategy to identify and filter the cases that do not.**

We sampled a set of 1000 domains from Alexa top 1M list. This sample was resolved from three vantage points Turkey, USA and Russia, and the resulting ip addresses were traceroute using TCP, ICMP and HTTP protocols, using an upper hop count threshold of 25. (All of these measurements were already completed previously) Using our custom analysis script, the common webservers across the vantage points and their corresponding traceroutes were then extracted and the rest of the data was discarded. This resulted in 504 common webservers. Then another level of filtering was applied, which was to only consider those webservers for which we received a reply and that to from the server in question, for all of the three protocols. This resulted in vantage point specific filtered list, due to our 25 hop threshold, not every common webserver in the list was reachable from all the vantage points. Therefore, for each list we computed for how many webservers the path lengths of protocol X and Y are exactly same (when probing the same server in question): for example, X=ICMP and Y=TCP path length were exactly same (labeled as ICMP-TCP in Table 3) for Russia, 206 times out of 296 successful traceroutes. The last column represents count of same path length for all three protocols combined.

From a high level view, Table 3 represents ICMP and HTTP path lengths differ more as compared to ICMP-TCP or HTTP-TCP. The difference in HTTP-TCP path length is mostly due to receiving RST packets from the server during HTTP traceroute, which would terminate it prematurely. Same logic is applicable for ICMP-TCP path lengths being more similar (having a higher count in table) than the ICMP-HTTP path lengths. On average 65% of the times all three protocol path lengths were exactly same, according to the last column of the table.

### 1.2 Reference (ICMP) Path Validation

- So and so papers have shown that routers and servers can block ICMP probes. We first establish the rate of such blocking (manifested by incomplete paths).
- Experiment: For a sample of top Alexa websites (10K), check reachability (path completeness and path inflation) to their authoritative name-servers and webservers over ICMP.
- *Path inflation:* Mention how we discover it: we started with TTL of 25 and were getting a high percentage of incomplete paths. Increasing the TTL to 64, increases the coverage of complete paths, but inflates it.
- Show empirical results and build an argument for discarding incomplete and inflated paths.
- Confirm that this happens from all vantage points.

### 1.3 Path Validation Data Collection

We decided to use Alexa Top 1M list, and randomly selected top 1000 domains from 100000 top domains. We did this to ensure that our current sample has sufficient variability with respect to where the servers are hosted, and who these servers belong to. For example, there a lot of www.google.** domains in top Alexa domains.


*Conference'17, July 2017, Washington, DC, USA*

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

We firstly resolve those 1000 domains using a custom resolver code[Link code's repo]. We used, this custom script and not the local resolver to make sure that the authoritative server of that domain replies to our IP rather than our local resolver's IP which move out of our domain of control. So this step was taken to ensure repeatability. This resolver code takes in a list of of domains and returns a file which has data in the following format.

domain, cname, authserverIP, webserverIP

We then divide the list into two sets, one set contains the list of domain and its corresponding authserverIP and the second set contains the list of domain and its corresponding webserverIP. We currently have rented four servers located at following locations:
1. USA
2. Russia
3. Turkey
4. China

Unfortunately we were unable to run any measurement beyond resolution on Chinese machine primarily because its a CentOS machine and we had to recompile a lot of scripts for that particular environment. With that said, we were able to resolve and run measurements from those three vantage points and collect data.

We ran a couple of preliminary measurements and found out that a lot of ICMP probes were not reaching the server, so our primary hypothesis was that most of the path were getting inflated because of IDS. So proposed way to measure this was to send ICMP packets with a higher TTL value so that IDS cases get eliminated and we have a solid set of paths onto which we can base our methodology.

So in this experiment, as mentioned earlier we would run two different set of traceroutes on different sets of resolved servers. For the Authoritative server we will send ICMP and UDP (DNS packets with query to get current bind version) probes. For Webservers we will send ICMP, TCP and HTTP packets. We set the intial max TTL value to be default traceroute value which is 25, and then we collected the results and analyzed them and then ran the same experiment with max TTL value of 64. For both the experiments if we do not receive a response for 15 consecutive hops, we terminate the traceroute.

We made a couple of assumptions in our analysis, first of all we assumed was in path inflation code. We assumed that if there are more than two non responding consecutive IPs in the traceroute we assumed that the path is inflated because of IDS.

Secondly, we are assuming that if there is no reply for fifteen consecutive hops then the server will not respond for the max ttl value either. Which essentially implies that IDS is completely blocking our access.

Before we go into the analyzing the results, we will first enlist the base numbers to give weight to the percentages.

In Russia there were a total of 805 unique webserver, and 869 unique authservers. In USA there were a total of 793 unique webserver, and 871 unique authservers. In Turkey there were a total of 788 unique webserver, and 867 unique authservers.

On a very high level, the results show a difference in percentage of ICMP probes that reach the server. On average around 85 percent of ICMP probes with TTL 25, and 98 percent ICMP probes when TTL value is 64, reach authoritative servers. Similarly, for in case of webservers we saw roughly equal reach-ability of about 75 percent for both 25 and 64 TTL.

There was a significantly higher path length inflation in ICMP paths to authservers compared to webservers (average of 25 percent vs 10 percent).

Broadly speaking, the TTL configuration of 64 with 15 gap limit would be ideal way to probe both webservers and authoritative servers, however there is a much higher incidence of ICMP blocking around webservers compared to authservers. In worst case we would be dropping around 20 percent of ICMP probes (if we dont fix the path inflation) for webservers and around 35 percent in case of authservers.

From a high level view, the data shows that there were roughly half the number of vantage points who had same server replying to all the vantage points, this counters the previously made assumption regarding the prevalence of CDNs in the list (at least for the vantage points we currently have). With that said, there was a roughly equal number of servers that were doing some degree of ICMP blocking based on the geo-location 11 in Authservers and 12 in Webservers. The non replying servers across the VPs suggest that we have ICMP blocking implemented at those servers and they should be filtered before we start our actual measurement phase.

While analyzing the IPs reachable from one or two vantage points, first major observation was that these IPs were reachable using traceroutes and not using ZMap. This is counter-intuitive because scamper's probes are under more restrictions compared to ZMap's probes (15 gap limit). The second major observation was that even for some cases even if the ICMP probes were not reaching the end host, the TCP probes were reaching the end host. Specifically in case of russian vantage point, in which the TCP packets were getting intercepted by a server close by (6th hop from the VP) and the ICMP probes were reaching on average thirteen hops before getting lost in the abyss.

## 1.4 Inflated Paths - Missing hops

Figure 1 shows the distribution of inflated paths for ICMP traceroutes that appear complete (we can reach server in question), but responses between hops are missing. The analysis has been carried on the list of nameservers that were common for all vantage points.

The results significantly vary among the vantage points due to the differences in path length in reaching the same server. For example, if a nameserver 'X' is 8 hops away from our vantage point in Russia and 12 hops away from our vantage point in USA. And an IDS is situated on path to the server which does not allow packets with lower than 14 ttl value to pass, then traceroute from Russia will have 6 missing hops whereas traceroute from USA will have 2 missing hop, for the same nameserver. This variance in path length is contributing towards the variation in CDF across vantage points.

| Vantage Point | Authoritative Nameservers Reachability | | | | Webservers Reachability | | | |
|---|---|---|---|---|---|---|---|---|
| | % Complete Paths | | % Possible Inflated Paths | | % Complete Paths | | % Possible Inflated Paths | |
| | TTL=25 | TTL=64 | TTL=25 | TTL=64 | TTL=25 | TTL=64 | TTL=25 | TTL=64 |
| Russia | 87.2 | 98.3 | 23.2 | 23.5 | 75.1 | 75.8 | 10.7 | 11.1 |
| Turkey | 84.3 | 99.5 | 33.2 | 36.5 | 75.6 | 78.0 | 9.9 | 11.9 |
| USA | 84.7 | 98.6 | 22.8 | 25.1 | 73.7 | 76.5 | 7.1 | 9.5 |
| China | NA | NA | NA | NA | NA | NA | NA | NA |

**Table 1:** ICMP reachability for Y websites. We start with the Alexa top 10,000. Filter down to the set that have the same authoritative name server from all vantage points, resulting in n = X. We further filter down to the set that have the same webserver across all vantage points, resulting in n = Y.

| Number of Vantage Points | Authoritative Nameservers (n=) | Webservers (n=) |
|---|---|---|
| None | 72 | 170 |
| Only one | 3 | 4 |
| Only two | 8 | 8 |
| All Three | 437 | 383 |

**Table 2:** ICMP reachability for Y websites using three back-to-back ICMP probes (TTL = 64). We start with the Alexa top 1,000. Filter down to the set that have the same authoritative name server from all vantage points, resulting in n = X. We further filter down to the set that have the same webserver across all vantage points, resulting in n = Y.
**X=520 and Y=565**

## RESULTS
## ANALYSIS
## DISCUSSION
## CONCLUSION
## REFERENCES

**Table 3:** Path Length Analysis

| Vantage Point | Common Nameservers across VPs (Y) | | | | | | |
|---|---|---|---|---|---|---|---|
| | < Neg One | Neg One | Same Length | One Hop Difference | Two Hop Difference | Three Hop Difference | > Three Difference |
| Russia ($Z_r$=940) | 27 | 36 | 671 | 35 | 23 | 1 | 8 |
| Turkey ($Z_t$=643) | 45 | 55 | 434 | 61 | 11 | 8 | 13 |
| USA ($Z_u$=738) | 30 | 59 | 603 | 41 | 2 | 0 | 3 |

Started with a random sample of Alexa domains and extracted their auth nameservers. Filtered down to the set that have the same nameservers from all vantage points resulting in n = Y. Further filtered down the set of nameservers for which the server in question replied, for both udp and icmp, resulting in $Z_i$, specific to each vantage point.
**Y=1000**. Shoaib : I didn't use these parameters -> Using 64 tll hop limit and 15 hop gap limit, the traceroutes were carried out with scamper.
**643** nameservers in Turkey were DNS and ICMP alive among 903 authoritative server. **940** in Russia and **738** in US were DNS and ICMP alive among 1000 authoritative servers

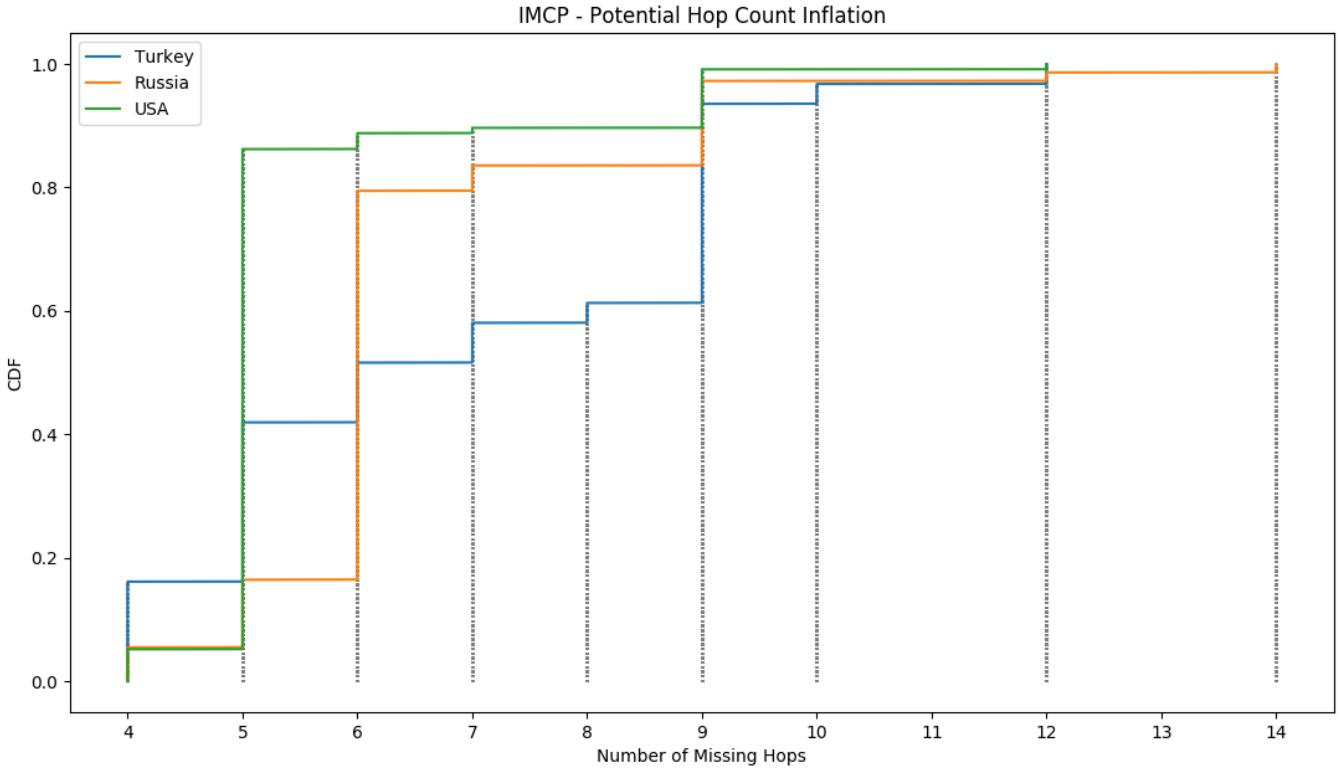


**Figure 1:** Distribution of path length inflation at *n* non-responding hops for 520 common nameservers across all vantage points. Following is the breakdown of number of nameservers for each vantage point:

US = 116
Turkey = 31
Russia = 73

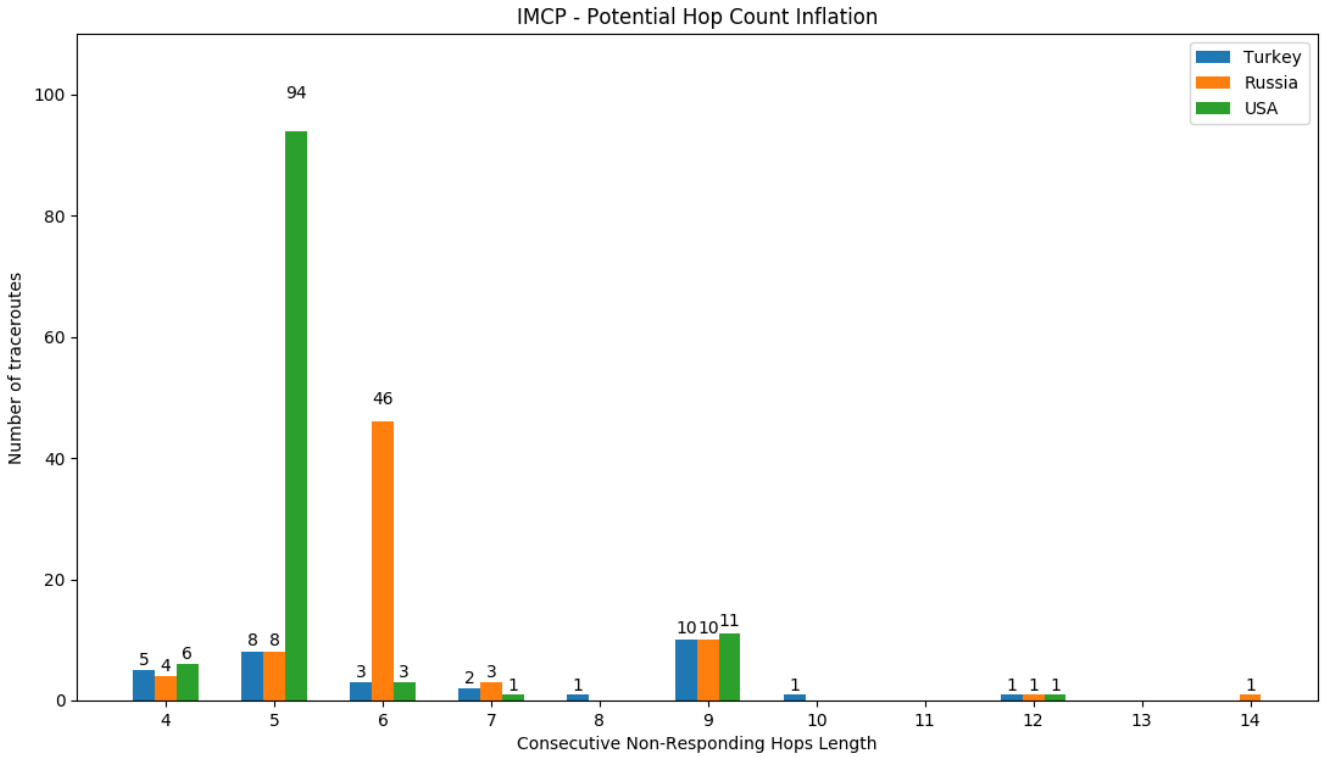


**Figure 2:** Bar plot of path length inflation in ICMP traceroutes for 520 common nameservers across all vantage points. The x-axis represents the number of consecutive non-responding hops $n$ and the y-axis shows the frequency of ICMP-traceroutes which have those $n$ length non-responding hops.