Location Matters: Eliciting Responses to Direct Probes

Ethan Blanton[†], Mehmet Engin Tozal[§], Kamil Sarac[‡], Sonia Fahmy[†]
[†]Purdue University, [§]Univ. of Louisiana at Lafayette, [‡]Univ. of Texas at Dallas
E-mail: elb@psg.com, metozal@louisiana.edu, ksarac@utdallas.edu, fahmy@cs.purdue.edu

***Abstract*—In this work, we propose techniques to attain visibility into an arbitrary Internet subnetwork that is responsive to indirect probes but *not* to direct probes. By probing the network from a small number of selected vantage points, we are able to collect information about network-layer topology which would otherwise be hidden from measurement due to rate limiting practices, security mechanisms, and routing dynamics. We investigate the reasons for differing visibility, and the required number and placement strategies of vantage points needed to collect topology information at a low cost. We demonstrate substantial improvement in global visibility as probed by the TraceNET path measurement tool when leveraging only five vantage points selected according to route similarity.**[1] [2]

I. Introduction

Studying topological characteristics of the Internet has been the subject of extensive research by the Internet measurement community [10, 22]. Results from these studies have been instrumental in understanding both structural and operational characteristics of the Internet. Implications of the network topology on (i) the design of distributed applications, (ii) the placement of services and data centers, and (iii) the development of Internet protocols, are well-documented. Additionally, researchers always need realistic topologies for their simulation, emulation, and testbed experiments, and operators are always seeking tools to aid in debugging network problems [16].

Topology measurement studies typically involve collecting raw connectivity data and processing them to build the corresponding topology maps at various levels of resolution, with the Autonomous System (AS) level, interface (*i.e.*, IP address) level, and router level being the most commonly studied levels. There has been recent interest in extending the scope of topology measurement research to include subnetwork (subnet) structures, since subnets are important building blocks of the Internet topology at the network layer [18, 24].

Topology mapping studies often employ *active* probing to collect raw topology data. Active probing schemes can be divided into two categories: *indirect* probing (such as the targeted generation of ICMP Time Exceeded messages used by `traceroute`-style methods to identify router addresses [14]), and *direct* probing (such as sending ICMP Echo Request messages [19] or TCP SYN segments [25] directly to an address of interest). It has been reported that the responsiveness of routers to active probes may exhibit differences based on the source (*i.e.*, the vantage point) of the probe messages as well as the type of the probe messages, *i.e.*, whether they are direct or indirect probes [12].

Internet topology maps are constructed by merging multiple partial views collected by means of a set of distributed vantage points. However, each vantage point involves significant amounts of query/response packets, necessary to build a partial view of the Internet. Moreover, these partial views overlap, oftentimes to a significant degree, resulting in unnecessary use of resources and attenuated coverage.

In this paper, we propose (i) techniques for increasing network visibility with active probing, and (ii) approaches for selecting a small set of vantage points to achieve high network coverage with minimum resource overhead. More specifically, we present heuristics to select a small number of vantage points to probe *an arbitrary subnet* using direct probing techniques *at minimal cost* (in terms of probe packets) with high probability of success. We use the task of collecting subnet information — the range of IP addresses assigned to the interfaces on each subnet visited on the path between two nodes in the Internet — as a running example of our methodology. Our approach, however, is also applicable to other active probing-based topology measurement tasks, such as active probe-based IP alias resolution as implemented in Ally [23].

Because we are choosing vantage points for *wide-scale mapping*, there is not necessarily any single "best" vantage point for this task, as there may be when probing a single, well-defined subnet. A related topic is the selection of vantage points for probing a *specific* subnet, AS, or local topology, but we defer this to future work.

We find that a subnet lying on a path to a destination may *not* be discovered from a given vantage point, but the same subnet may be discoverable from another vantage point. As an example, during the initial subnet exploration phase of our experiments, we found 588 such "hidden" subnets out of which 310 subnets were later successfully explored from other vantage points.

In addition, the visibility of interfaces on a subnet to indirect probing versus direct probing may differ. These differences may be due to firewalls or other middle boxes, router configuration, or routing dynamics. Specifically, a router may respond to indirect probes from a particular host, but that host may be

[1]The data sets and tools used in this paper can be downloaded from PURR at: https://research.hub.purdue.edu/projects/vantages

[2]This research has been sponsored in part by the GENI Project Office (GENI project 1723).

unable to use direct probes to query the router or its subnet. We explore the reasons for this via active probing and analysis of ICMP responses, as well as analysis of BGP advertisements. We then present approaches for selecting vantage points for probing arbitrary networks to achieve higher global visibility. Our objective here is to identify *a small number* of vantage points to maximize the probability of discovering any given subnet. At the same time, we wish to *limit the number of probe packets* which can overload the network and trigger security and rate limiting mechanisms against our measurement process itself.

The rest of this paper is structured as follows. Section II defines the problem. Section III demonstrates its prevalence. Section IV discusses some of the reasons for differing visibility. Section V describes methods for vantage point selection and Section VI gives our experimental results. We review related work in Section VII and conclude in Section VIII.

II. The Hidden Subnet Problem

We call a network that fails to respond to direct probes from a particular vantage point a *hidden subnet* with respect to that vantage point. We posit that some hidden subnets may be successfully explored via direct probes from alternate vantage points, and that we can heuristically identify such alternate vantage points. Such subnets may be reachable from only some portions of the Internet, or configured not to respond to direct probes from some hosts or networks, or located behind a firewall or other filtering device. In some cases, we expect that a vantage point can be found that circumvents the routing situation, administrative configuration, or filtering that prevents a given host from exploring a subnet that is hidden to it. Adding vantage points to a measurement process, therefore, may expose larger portions of the Internet topology to direct probes.

When selecting vantage points, there is a tension between measurement accuracy and cost. Since we are dealing with active measurements, each probe of a hidden subnet from any vantage point involves the emission of one or more packets toward the hidden subnet. Sending a large number of measurement packets toward a subnet in a short period of time consumes network resources that could otherwise be used for other traffic, and may trigger rate limiting or security mechanisms against our measurement process itself. Spreading the packets out over a long period of time minimizes short-term impact on the subnet being explored, but increases the probability that changes in Internet topology will take place during the probing process. Therefore, we wish to limit the *number of vantage points* to control cost and to perform the measurements over a relatively *short time period* (seconds to minutes) to preserve stability.

III. Hidden Subnet Characteristics

We use the TraceNET measurement tool [24] to illustrate differences in network visibility between direct and indirect probing methods. TraceNET ideally discovers and reports the IP addresses assigned to the interfaces on each subnet it visits on the path from the measurement host to a given destination host. TraceNET uses indirect probes in a manner similar to `traceroute` to identify routers along this end-to-end network path. It then sends direct probes to each router discovered by indirect probing and the addresses adjacent to it. The responses to these probes are used to map the subnets along the path. Some portion of these routers which were discovered by indirect probing, and/or their adjacent addresses, do not respond to the direct probes. If no address adjacent to a router responds to direct probing, TraceNET reports the subnet as a subnet comprising only the router itself (that is, a single IP address with a 32-bit "slash 32" subnet mask), as no information about the subnet was successfully gathered. These networks which fail to respond to direct probes are the *hidden subnets* from Section II. While we are able to glean the existence of these subnets, their details are hidden from the host's direct probes and we are unable to determine any additional configuration information.

The disparity between reachability via direct and indirect probing from a single vantage point is a known problem [12]. In this work, we address the responsiveness of routers on a subnet to direct probes from multiple vantage points. For our case study of subnet mapping, we are further concerned with the responsiveness of *hosts lying on a particular subnet*, rather than simply the ingress and egress points of that subnet. To quantify the occurrence of hidden subnets, we collected a data set comprising the output of the TraceNET tool from 200 diverse PlanetLab [8] hosts. Each host runs TraceNET toward twenty other hosts selected uniformly at random from the other hosts, for a total of 4,000 TraceNET invocations.

Out of the 4,000 TraceNET invocations, 55,621 subnet records and 5,122 "anonymous" hops were identified (anonymous hop means that no ICMP Time Exceeded message was returned for that TTL, and so TraceNET could collect no information about the subnet at that hop). We do not consider the anonymous hops further in this paper. As expected, many subnets appear on multiple paths and 55,621 subnet records in our data set contribute to 2,818 distinct subnets.

We found 588 distinct hidden subnets (subnets with a single IP address that could not be further explored) in this data set, or about 21% of the 2,818 identified subnets. Of the 4,000 end-to-end paths probed by TraceNET, over 70% (2,842) contained at least one hidden subnet, with a median of 2 hidden subnets per path (mean 2.9, standard deviation 2.9). Of those 588 hidden subnets, 310 were successfully explored from some other location in the network on another path in this data set, demonstrating the potential for increased visibility from leveraging additional vantage points.

IV. Reasons Hidden Subnets Occur

We conducted experiments to gain insight into the reasons that the routers in hidden subnets are unresponsive to active probes. Based on our observations below, the two most likely reasons for unresponsiveness are administrative configurations and routing issues.

Network operators may choose to implement different policies with respect to direct and indirect probes. Given that indirect probes are commonly used in `traceroute`-based network debugging, there may be a collective incentive to support them. In contrast, direct probing is considered more intrusive and hence may be subject to administrative blocking by network operators. Routing decisions may also play a key role in causing hidden subnets, where an IP address discovered via indirect probing from a vantage point may not be reachable by the same vantage point or may not be reachable at all, *i.e.*, its address block may not be advertised via BGP.

A. The `dallastr` Tool

In this section, we present a tool, called `dallastr`, that we developed and used to collect information on router responsiveness. `dallastr` is a slightly modified version of `traceroute` and provides a more detailed level of information about router responsiveness. `dallastr` sends an ICMP Echo-Request probe to each IP address discovered during the `traceroute` session and records the type and code of the returning ICMP response (if any) along with the IP address of the router sending the ICMP response.

Fig. 1 presents an example output of `dallastr` run at a vantage point with IP address 130.216.1.23 toward a destination node with IP address 139.19.142.5. In this trace, the 17 IP addresses in the middle section of the table are discovered by indirect probes. Each of these IP addresses are sent ICMP Echo Request direct probes (with TTL 255), and the returned ICMP response type and code are recorded along with the IP address of the router issuing the response in the third section of the table. In this table, the IP address discovered at hop distance 5 via indirect probing cannot be probed via direct probing, eliciting no response, denoted by a '*' entry in the output. Similarly, direct probes to the IP addresses discovered at hop distances 10 through 16 cannot be completed, resulting in ICMP Destination Unreachable / Communication Administratively Prohibited (3/13) error messages or no response. Note that the IP address discovered at hop distance 10 responds to the direct probe by returning an ICMP (3/13) error message from the IP address probed, rather than returning an Echo Reply message.

B. Classification of Records

We used our PlanetLab data collection setup to run `dallastr` and collect data on 4,000 end-to-end paths. A small portion of the paths may be represented in both directions as separate collections.

The data set includes a total of 61,109 records where a record corresponds to a single line in the output of the `dallastr` tool. The breakdown of the records based on the returned information is classified as shown in Fig. 2. In the figure, Set ***A*** includes 55,381 records where routers are responsive to indirect probes. These are the records where the "Discovered IP" column in Fig. 1 includes an IP address rather than a '*'. In the other records, routers do not respond to indirect probes. Set ***A*** includes 2,757 unique IP addresses.

Set ***B*** includes 47,817 records where a direct probe to indirectly discovered IP address returns a response. These are the records where "ICMP Source" column in Fig. 1 includes an IP address rather than a '*'. Set ***B*** includes 2,614 unique IP addresses. Out of this set, 46,409 records are for cases where the response comes back from the probed IP address (Set ***C***) and in 1,408 records the response comes back from some other IP address (Set ***D***).

Set ***C*** includes 2,572 unique IP addresses. Set ***D*** includes 75 unique IP addresses which were the destinations for direct probes but the responses come from some other IP addresses. In Set ***C***, 45,992 records are for cases where routers return ICMP (0,0) Echo-Reply message (Set ***E***) and 417 records are for cases where routers return ICMP (3,13) Administratively Prohibited message (Set ***F***) instead of an ICMP (0,0) Echo-Reply. Set ***F*** includes 7 unique IP addresses contributing to 417 records.

In Set ***D***, 1,295 records return an ICMP (3,13) Administratively Prohibited response (Set ***G***); 65 records return ICMP (11,0) TTL Expired message (Set ***H***); 4 records return ICMP (3,0) Network Unreachable message (Set ***I***); and 44 records return a ICMP (3,1) Destination Host Unreachable message (Set ***J***). In Set ***J***, ICMP (3,1) responses come from 13 IP addresses belonging 4 different domains including Pacific Wave Gigapop, OpenTransit Backbone, QWest, and EP.NET.

In the ICMP (3,13) cases (Sets ***F*** and ***G***), most of the records are generated by routers in European networks (except for about 50 records generated by AT&T routers and about 140 records generated by Jordan Telecom routers). In about 1,260 of these records, we observe GEANT routers returning ICMP (3,13) record for directly probed IP addresses within GEANT or DFN.DE domains.

In 8,972 cases, direct probes to IP addresses either did not result in a response (Set ***K*** with size of 7,564 records) or responses came from some other IP address (Set ***D*** with size of 1408 records). Of the 7,564 records in Set ***K***, direct probes to 376 distinct IP addresses resulted in no response when probed from a vantage point. Out of these, 203 IP addresses responded when probed from some other vantage points.

We observed cases where a direct probe to an IP address resulted in different types of responses. As an example, when an IP address in `uni-paderborn.de` domain was probed from a vantage point in the `cs.washington.edu` domain, it returned no responses; when probed from a vantage point in `cesnet.cz` domain, it returned ICMP (3,13) Administratively Prohibited and when probed from a vantage point in `mpi-sws.mpg.de` domain, it returned ICMP (0,0) Echo Reply.

C. BGP Correlation

We correlated the 2,757 IP addresses identified in Set ***A*** from Section IV-B with Route Views [2] BGP RIBs from the six Route Views vantage points having sizeable data sets for the date in question: University of Oregon, Equinix Ashburn (Ashburn, VA), ISC (Palo Alto, CA), LINX (London, England), PTT Metro/NIC.br (Sao Paulo, Brazil), and Equinix

		Indirect Probe				Direct Probe		
Source	Destination	Hop Dist.	ICMP TYPE	ICMP CODE	Discovered IP	ICMP TYPE	ICMP CODE	ICMP Source
130.216.1.23	139.19.142.5	1	11	0	130.216.1.125	0	0	130.216.1.125
130.216.1.23	139.19.142.5	2	11	0	210.7.32.1	0	0	210.7.32.1
130.216.1.23	139.19.142.5	3	11	0	210.7.36.227	0	0	210.7.36.227
130.216.1.23	139.19.142.5	4	11	0	210.7.36.186	0	0	210.7.36.186
130.216.1.23	139.19.142.5	5	11	0	207.231.240.131	*	*	*
130.216.1.23	139.19.142.5	6	11	0	64.57.28.97	0	0	64.57.28.97
130.216.1.23	139.19.142.5	7	11	0	64.57.28.113	0	0	64.57.28.113
130.216.1.23	139.19.142.5	8	11	0	64.57.28.7	0	0	64.57.28.7
130.216.1.23	139.19.142.5	9	11	0	62.40.125.17	0	0	62.40.125.17
130.216.1.23	139.19.142.5	10	11	0	62.40.124.34	3	13	62.40.124.34
130.216.1.23	139.19.142.5	11	11	0	188.1.145.37	3	13	62.40.124.34
130.216.1.23	139.19.142.5	12	11	0	188.1.145.90	3	13	62.40.124.34
130.216.1.23	139.19.142.5	13	11	0	188.1.145.85	*	*	*
130.216.1.23	139.19.142.5	14	11	0	188.1.145.102	3	13	62.40.124.34
130.216.1.23	139.19.142.5	15	11	0	188.1.145.97	*	*	*
130.216.1.23	139.19.142.5	16	11	0	188.1.234.38	3	13	62.40.124.34
130.216.1.23	139.19.142.5	17	11	0	134.96.6.28	0	0	134.96.6.28
130.216.1.23	139.19.142.5	18	0	0	139.19.142.5	0	0	139.19.142.5

Fig. 1. A sample `dallastr` output

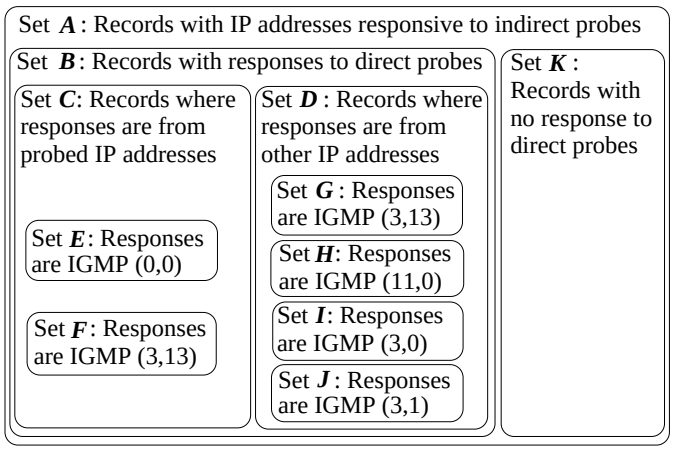


Fig. 2. `dallastr` result breakdown.

Sydney (Sydney, Australia). For each IP address, we identify all prefixes in the six RIBs containing the address, and determine whether the address is routeable from all vantage points, some vantage points, or whether no valid AS path is found. Unfortunately, due to the nature of BGP and the limited data available to us, we have no way to determine what the path between two vantage points was according to the BGP rules within the source vantage point's AS, so we cannot draw conclusions about specific BGP routes.

We find that 2,354 addresses belong to a prefix with a valid AS path in all six RIBs. We cannot determine if these paths are globally routeable, as there may be ASes from which they have no valid path, but we can conclude that they are directly reachable from broad swathes of the Internet. Of these addresses, 2,267 appear in Set ***B***, and 282 appear in Set ***K*** (195 appear in both sets, from different vantage points).

There were 312 addresses that appeared in some, but not all, of the six RIBs. It would appear that these addresses are not globally routeable, at least from the point of view of the Route Views vantage points we observed. Of these, 278 appear in Set ***B***, 57 appear in Set ***K***, and 25 appear in both from varying vantage points.

Finally, 91 of the addresses in Set ***A*** do not appear in any of the six BGP RIBs. Of those, 31 are RFC 1918 [21] private addresses, which are never globally routeable. From the remaining 60 IPs, 43 appear in Set ***B*** and 26 in Set ***K***. Only 9 appear in both sets.

D. Summary of Results

In summary, the records in Set ***K*** suggest that either (1) the routers are configured to ignore, filter out, or selectively respond to ICMP Echo Request messages, or (2) there is no route from the vantage point to the probed IP address. We consider the former case as evidence of administrative configuration issues and consider the latter case as evidence of routing issues. Analysis of BGP advertisements from the date of data collection suggests that some proportion of the addresses in Set ***K*** were not present in the BGP routing database from RouteViews. However, while the limitations of our data set preclude confirming global routeability, some IP addresses in Set ***K*** appear to be widely reachable, if not globally routeable, suggesting filtering. In addition, the records with ICMP (3,13) responses (Sets ***F*** and ***G***) can be seen as evidence of administrative configuration issues causing non-responsiveness.

The records in Sets ***H***, ***I***, and ***J*** suggest routing issues such as possible routing loops (due to ICMP (11,0) messages) or lack of routes toward the directly probed IP addresses (due to ICMP (3,0) and ICMP (3,1) messages). Furthermore, the fact that 203 IP addresses in Set ***K*** are reachable by some vantage points but not all also suggests that routing issues cause partial visibility, which is confirmed by our observation that 57 of the

IP addresses in Set ***K*** had partial BGP visibility in the Route Views data set.

Ultimately, 2,516 of 2,720 public IP addresses discovered via indirect probes were reachable via direct probes from *some* vantage point in this experiment. This motivates the need for probing from multiple vantage points.

V. Selecting Vantage Points

We established in Section III that visibility to direct probes varies by vantage point. In Section IV, we showed that most of the hidden subnets we encounter are due to administrative configuration or routing issues. We now turn to the problem of identifying vantage points that may circumvent these administrative or routing restrictions to give us broad visibility into Internet subnetworks.

We first define a baseline process for randomly selecting vantage points and evaluating their efficacy in increasing visibility into arbitrary Internet subnets when using direct probes. We then describe four heuristics for selecting a small number of vantage points for maximum visibility at little cost.

A. Baseline: Selecting Vantage Points at Random

For a baseline with which to compare vantage point selection heuristics, we first consider randomly-selected vantage points. We select thirty vantage points uniformly at random from among all hosts participating in the experiment independently for each hidden subnet we wish to explore. We then use these hosts to probe the hidden subnets for which they were selected.

This selection method represents the results one would expect when choosing arbitrary Internet hosts to perform direct measurement. We will compare our methods for vantage point selection to these results to evaluate their effectiveness in choosing vantage points which provide high visibility.

B. The RSIM Route Similarity Metric

For three of our vantage point selection methods, we employed the RSIM [13] route similarity metric. This unitless metric describes "the overlap of two end-to-end routes between two nodes and an arbitrary third node," aggregated for a set of reference destinations. Computation of RSIM is defined as:

$$RSIM(s_1, s_2, SET) = \frac{\sum_{d \in SET} 2 \cdot \mathrm{Common}(s_1, s_2, d)}{\sum_{d \in SET} \mathrm{Total}(s_1, s_2, d)}$$

In this equation, s_1 and s_2 are vantage points, and SET is a set of destination IPs. $\mathrm{Common}(s_1, s_2, d)$ is defined as the number of hops which exist on both the measured path from s_1 to d and the measured path from s_2 to d. Similarly, $\mathrm{Total}(s_1, s_2, d)$ is defined as the total number of hops in each of the two paths added together. The precise computation of $\mathrm{Common}(s_1, s_2, d)$ was not given in [13], but we used the length of the longest common subsequence between s_1 and s_2.

C. By AS Degree

On the hypothesis that hosts homed in Autonomous Systems (ASes) with a large number of neighbors are likely to exhibit significant route diversity, this method selects vantage points by AS neighbor degree. We select vantage points that belong to the ASes having the highest AS neighbor degree according to current BGP advertisements. We call this method of vantage point selection **ASDegSel**.

D. By Traceroute-based RSIM

For this selection method, which we call **TrRSel**, we compute RSIM for every pair of vantage points as described above. Working again on the assumption that diversity in probe routing will help us avoid routing problems and administrative filters, we use RSIM to choose the set of vantage points that have the minimum total route similarity among them. In other words, to select k vantage points, we choose the vantage points $V = \{v_1 \ldots v_k\}$ that minimize

$$\sum_{v_i \in V} \sum_{v_j \in V - v_i} \mathrm{RSIM}(v_i, v_j, SET).$$

E. By AS-based RSIM

This selection method, **ASRSel**, uses RSIM to choose the set of vantage points having the minimum total AS path similarity among them. We did not have access to the BGP tables *from* each vantage point. In [13], the authors found that RSIM predicted reverse routes as well as forward routes, so we use this property to select hosts based on their AS routes.

We use the same routing database as the AS degree computation in ASDegSel to find all known AS paths *to* each vantage point from a Route Views monitor, and use these paths to compute RSIM between each pair of vantage points.

F. By TraceNET-based RSIM

Extending RSIM to TraceNET paths, this selection method chooses the set of vantage points having the minimum total TraceNET path similarity among them. We call this method **TNRSel**. To perform RSIM on TraceNET paths, we define $\mathrm{Common}(s_1, s_2, d)$ across subnets, rather than IP addresses. A TraceNET-discovered subnet in the path from s_1 to d is considered a match for a subnet in the path from s_2 to d if they have the same base address and netmask length, or if one is contained within the other. The route similarity among selected hosts is then minimized in the same manner as the `traceroute`-based RSIM in TrRSel.

VI. Evaluation

Now that we have defined a baseline selection method and proposed four selection methods, we experimentally compare them for efficacy in providing visibility to direct probes.

We say that a hidden subnet is *exposed* by a vantage point if the vantage point is able to probe the hidden subnet and identify more than one host that lies on that subnet per the heuristics defined by TraceNET. Note that we are only interested in whether a hidden subnet is exposed or not. For our purposes, a set of vantage points that *exposes* more hidden

subnets is superior to a set of the same size that exposes fewer hidden subnets.

Each experiment in this section selects potential vantage points from a set of 200 PlanetLab [8] hosts. We compare the effectiveness of the four selection methods by comparing the hidden subnets they are able to expose to the hidden subnets exposed by a baseline experiment. The hidden subnets used for evaluation are drawn both from paths between PlanetLab hosts and from paths between an Internet host at Purdue University and hosts in the public Internet selected from the Alexa Top 500 Global Sites [3] index.

A. Methodology

The 200 PlanetLab hosts used as potential vantage points were chosen uniformly at random from the set of all available PlanetLab hosts that were up and running and able to complete a small number of functionality tests on the date of the experiment. They are the same hosts used in Section IV.

Experiment setup involves mapping the routes between vantage points and identifying hidden networks. The route maps are required for the computation of the RSIM metrics and the hidden networks provide our measure of success. All-pairs `traceroutes` were taken between the 200 potential vantage points, as well as 20 TraceNETs from each potential vantage point directed toward 20 other vantage points selected uniformly at random from the remaining 199. We therefore collected 39,800 `traceroutes` and 4,000 TraceNET measurements in this step.

As described in Section III, we identified 55,621 subnets and 5,122 "anonymous" hops, with 2,818 unique subnets, on 4,000 TraceNET-probed paths. 588 of these subnets were hidden. These 588 hidden subnets constitute the set of subnets that we will attempt to expose in the rest of this section.

B. Reasons for Identified Hidden Subnets

The reasons behind hidden subnets, along with some data illuminating the prevalence of certain conditions in the paths explored by our data set, were discussed in Section IV. We now analyze the 588 hidden subnets identified in Section VI-A, which we will use for evaluating vantage point selection methods in the rest of this section.

Analysis of data reported by the `dallastr` tool in Section IV-B classified 289 of the 588 hidden subnets into Set ***E***, indicating that a `dallastr` probe was able to send an ICMP Echo Request packet to the address and received an ICMP Echo Reply. An additional 277 are in Set ***K***, indicating the vantage point running `dallastr` was unable to elicit a response to a direct probe sent to the hidden subnet address.

Of the remaining 22 addresses, 11 were not present in the `dallastr` data set. This could be due to route changes between back-to-back probes (`dallastr` and TraceNET were run temporally close together during data collection, for each pair of hosts), ICMP rate limiting, differences in treatment between TCP and ICMP traffic, or simple packet loss.

Six of the final 11 addresses were classified into Set ***F***, Administratively Prohibited, 4 into Set ***H***, TTL Expired, and one into Set ***I***, Network Unreachable.

This suggests that the hosts in Set ***E*** have only partial reachability with reasonably high confidence; Sets ***H*** and ***I*** are routing misconfigurations or transient errors with high confidence; and Set ***F*** is hidden due to administrative configuration with high confidence. The 277 hosts in Set ***K*** give us little information as to the nature of their lack of response to direct TraceNET or `dallastr` probes.

The Route Views data discussed in Section IV-C reveals that 34 of the 588 hidden subnets have no route in any of the six RIBs. Of those 34, 6 are RFC 1918 [21] private addresses. All six RIBs contain 471 of the hidden subnets, suggesting that they are likely to be globally, or at least widely, routeable. The remaining 83 subnets are present in some, but not all, of the six RIBs, and are thus likely not globally routeable.

Interestingly, four hidden subnets which do not appear in any of the RIBs analyzed are exposed by at exactly two vantage points at the same physical location (Lawrence Berkeley National Laboratory) in the following sections. Three of the four addresses are on the same subnet, and the fourth is numerically similar. We must assume that, while they are not reachable networks from any of the BGP vantage points drawn from Route Views, the previously-mentioned limitations of this approach hide the fact that they are routeable from some portions of the network.

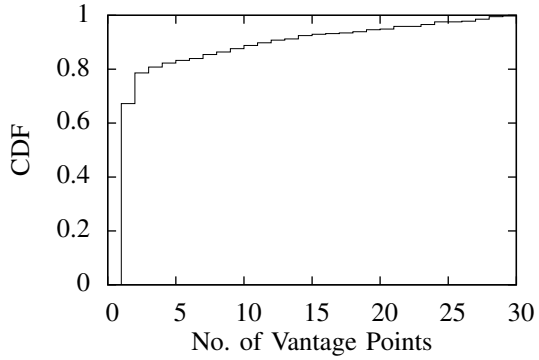
C. Random Vantage Selection

Having collected topology information and identified hidden subnets, we perform random vantage point selection as described in Section V. We then run the ExploreNET tool against the hidden subnets from their selected vantage points. ExploreNET is a sister tool to TraceNET that minimizes the required probe budget to discover a hidden subnet. Unlike TraceNET, it does not provide the complete path from the probing host to the destination.

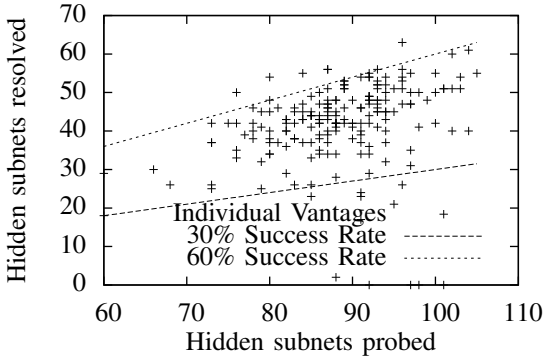
Out of the 588 hidden subnets probed in this data set, one or more vantage points exposed 412 subnets as larger than one host. The remaining 176 hidden subnets were hidden from all vantage points that attempted to probe them. Eleven of these remaining subnets were in private address space and as such are unreachable from all but local hosts by definition. The remainder of this section will consider only the 412 subnets that were hidden from some, but not all, of the vantage points.

For each of these hidden subnets, we calculated the number of randomly-selected vantage points required to expose that subnet. To do this, we randomly shuffled the thirty vantage points that probed the subnet, then iterated the resulting list to find the first vantage point that exposed the subnet. The index of this vantage point in the shuffled list represents the number of vantage points required to expose the subnet. For example, if the first four vantage points in this list could not expose the hidden subnet, but the fifth vantage point did, then we say that 5 randomly-selected vantage points were required to expose the subnet. Fig. 3(a) shows the cumulative distribution function of this data.

Recall that Fig. 3(a) contains only those 412 subnets that were visible to at least one vantage point. As illustrated in



(a) CDF demonstrating the number of randomly-selected vantage points required to expose those hidden subnets which proved resolvable.



(b) Hidden subnets probed versus hidden subnets successfully resolved for each vantage point.

Fig. 3. Performance of random vantage point selection.

the figure, 67% of these resolvable subnets were exposed by choosing a single vantage point at random and probing the hidden subnet. Adding additional randomly selected vantage points increases the number of hidden subnets that are successfully exposed, but the utility of these randomly selected vantage points falls off rapidly. Four such vantage points are required to expose 80% of the hidden subnets, 12 are required to expose 90% of the hidden subnets, and 21 to expose 95%.

Several experiments using different hosts and similar methodology yielded the same roughly logarithmic decay in marginal utility for additional vantage points. This suggests that the first few vantage points provide the most "bang for the buck," and that a small number of randomly-selected vantage points maximizes the trade-off between achieving desirable resolution of hidden subnets and minimizing the cost of measurement.

D. Vantage Point Success Rate

Within this data set of random vantage points, we also studied the *success rate* of the vantage points. We define the success rate of a vantage point as the number of hidden subnets exposed divided by the number of hidden subnets probed. We found that the success rate of vantage points varied considerably. Fig. 3(b) shows the success rate of each vantage point on a scatter plot. Most vantage points fall within a range of about 30% and 60% successful. The best-performing vantage point is about 70% successful, and the worst is under 20%. 103 of the 200 vantage points had a success rate of 50% or higher.

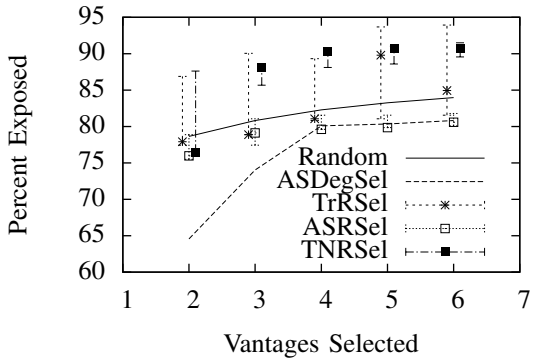


Fig. 4. Effectiveness of selected vantage points in percentage of hidden subnets exposed. Points represent the actual selection, error bars are the best and worst selections in the top 10 choices.

E. Comparing Selection Methods

The `traceroute` and TraceNET topology information from Section VI-A along with the success rates from Section VI-D provide us with the measurement data we need to compute our selection methods. For BGP and AS information, we used the Route Views [2] routing database from `route-views.routeviews.org`.

To perform AS degree selection via ASDegSel, we first locate the AS of a host by querying the routing database for the origin AS of its IP address. We then query the same database to count the ASes lying adjacent to this origin AS on all paths terminating at the origin AS, and use this as the degree for selection[3].

Because the RSIM selection methods described in Section V are n choose k operations, we make this computation more tractable by eliminating those vantage points that had a success rate (as computed in Section VI-D) of less than 55% before performing selection via the RSIM methods. In this data set, this leaves us with 43 hosts for the RSIM selection methods.

For each RSIM selection method, we then chose sets of 2 to 6 vantage points and identify the top ten sets for each size using the RSIM metric. Please note that, in practice, we would choose only the best-scoring set for a given size. However, because there may be several interesting sets, in this part of the experiment we would like to compare the *RSIM metric's best-scoring set* with some of the other highly scoring sets. Next, for each of these sets for each size, we experimentally test their effectiveness in exposing the hidden subnets.

Fig. 4 compares the effectiveness of the four selection methods described in Section V against the results of random selection of vantage points as described in Section VI-C. This

[3]Tie-breaking for ASes of the same degree is arbitrary.

TABLE I
MARGINAL UTILITY OF VANTAGE POINTS BY HIDDEN SUBNETS EXPOSED.

	V1†	V2†	V3	V4	V5
TNRSel	10	10	2	3	1
TrRSel	8	9	37	1	2

figure shows that TrRSel and TNRSel can perform markedly better than random selection. However, TrRSel shows significant inconsistency, with the poorest-performing of the top 10 best-scoring sets of vantage points performing more poorly than random selection in every case and the best-performing of these sets performing better than random selection in every case. In addition, the single best-scoring set (which is the one returned by our RSIM method) performs more poorly than random selection in several cases, *e.g.*, the 2, 3, and 4 node sets. TNRSel, on the other hand, displays much more consistent performance, with the single best-scoring selection also being one of the best-performing selections in every instance but the two-host selections. ASDegSel and ASRSel do not perform substantially better than random selection for any size selection, and in fact generally perform more poorly.

TNRSel provides an improvement over random selection of more than 7% in hidden subnet exposition when selecting 4-6 vantage points. TrRSel displays the potential to improve selection significantly, but has more erratic performance. Selecting 5 vantage points with either TNRSel or TrRSel performs as well as randomly selecting 12 or 11 vantage points, respectively, for this data set.

F. Marginal Utility of Individual Vantage Points

Section VI-E demonstrates that two of the selection methods from Section V perform better than random selection of vantage points. These selection methods are designed to identify collections of vantage points with mutually dissimilar views into the network. To evaluate this dissimilarity, we examine two sets of vantage points to determine the number of hidden subnets that are exposed by *only one* vantage point, as well as the distribution of these subnets among the vantage points. The two sets of vantage points are the best-scoring TrRSel and TNRSel sets of 5 vantage points. (These sets correspond to the points plotted in Fig. 4 above the 5 vantage points mark for the TNRSel and TrRSel curves, respectively.) There are a total of eight vantage points between these two sets, as two hosts appear in both sets.

Using TNRSel for vantage point selection, 401 subnets are exposed by the five vantage points. Of these 401 subnets, 269 are exposed by all five vantage points, and 25 are exposed by only one vantage point. TrRSel displays similar characteristics. The five vantage points selected via this method expose 399 total subnets, with 255 being exposed by all five vantage points and 53 exposed by only one vantage point.

Table I shows the marginal utility of each host in these two sets of vantage points in terms of hidden subnets exposed. Each column of the table represents one of the five vantage points in a given set, and each row a selection method. The vantage points are arranged in arbitrary order, with the two vantage points that appear in both sets, marked with the † symbol, appearing in the same column for both sets. It can be seen that the marginal utility of each individual vantage point is quite low, under 1% for the most productive single vantage point. This follows from Fig. 4, which shows that the expected utility of adding a single given vantage point is low.

G. Probing the Internet at Large

We now consider a data set based on the Alexa Top 500 Global Sites [3] index for October 19, 2011. For this data set, we first performed a TraceNET to each of the 447 unique IP addresses yielded by resolving the Alexa Top 500 web sites[4] from a single location at Purdue University. From this data we extracted 509 hidden subnets. We then probed each of these 509 hidden subnets from 30 vantage points selected uniformly at random from the PlanetLab hosts used in Section VI-A as well as from the best-scoring sets of vantage points used in Section VI-F. Eight vantage points failed entirely during the data collection process, and one host collected only partial data. None of these failed vantage points were in the best-scoring sets of vantage points.

Thirty probes to each hidden subnet from randomly selected vantage points exposed 188 of the 509 subnets. The remaining 321 were not exposed by any vantage point in this experiment. Using the methodology in Section VI-C, five randomly-selected vantage points would expose 146 hidden subnets.

The vantage points selected by the TNRSel method exposed 181 hidden subnets, and TrRSel exposed 179 hidden subnets. This represents 96% and 95% of the 188 subnets exposed by the complete random probe set, respectively, and the equivalent performance of 21 randomly selected vantage points. Despite the significantly higher proportion of subnets that cannot apparently be exposed from any vantage point in the experiment, the TNRSel and TrRSel methods maintain a significant advantage over random vantage point selection.

H. Implications

The experiments presented here represent one of several sets of experiments performed at different times and involving different vantage points. While the results from these sets of experiments differ in some respects, the results are broadly similar. The number of hidden subnets that are not exposed by any vantage point varies depending on the set of hidden subnets identified, and ranges from about 20% of all hidden subnets to 40% of all hidden subnets. In several scenarios, a large number of hidden subnets in a single AS that were not exposed by any vantage point were identified. One particular AS appears to administratively block ICMP probing of many routers within its networks entirely.

The performance of ASRSel and ASDegSel appears to be more volatile than TrRSel and TNRSel. However, while in several scenarios they perform as well as random selection, in no scenario do they perform substantially better than random selection. TNRSel and TrRSel, on the other hand, consistently

[4]Eight of the 500 domains did not resolve without additional subdomain or hostnames, and several of the other domains resolved to the same IP address.

perform markedly better than random selection, with 5 vantage points selected by one of these methods performing as well as 12-15 vantage points selected at random.

If about 70% of hidden subnets can be resolved from *some* vantage point (which corresponds roughly to our experiences, although some data sets, such as that in Section VI-G, are much lower and some are much higher), and five vantage points selected via our two best performing methods expose about 90% of these hidden subnets, then we can expect to expose more than 60% of all subnets that are hidden from any given vantage point. Furthermore, our experiences show that, like the data set in Section VI-A, about 20% of the subnets identified by TraceNET from a variety of vantage points are hidden. Taken together, this means that using our methods to select five vantage points yields a total improvement of exposing about an additional 10% of all subnets.

VII. Related Work

Our work examines the problem of network visibility differences during active probe-based topology discovery, and presents a technique to improve the success rate of this task by probing from multiple vantage points. This directly applies to recent work that uses TraceNET [24] – a `traceroute`-like active probing tool, to discover subnet structures. Subnet-level topology information has also been considered in several recent studies, *e.g.*, [4, 18]. Our approach would also improve the success rate of other active probe-based topology discovery schemes such as Ally [23] – a probe-based IP alias resolver.

Network visibility differences have also been examined from the routing perspective. Bush *et al.* [7] compared the visibility differences of the data plane and control plane at the inter-domain level. More recently, Yan *et al.* [27] compared BGP tables of 25 ISPs to understand the causes of control plane visibility differences in different parts of the Internet. Other related include the studies [9] and [20] where the authors consider minimizing the active probing overhead in diagnosing network reliability or network outage related problems in the Internet.

Reverse traceroute [16] utilized multiple vantage points to probe the path from an arbitrary host back to the host running reverse traceroute. Their tool, however, utilized all available vantage points and focused on topological overlap of end-to-end paths. Our method studies the number and placement of the vantage points in order to minimize probe impact on foreign hosts (reverse traceroute probes toward a host "owned" by the experimenter), and revolves around subnet visibility, rather than topological placement, of the vantage points.

The Archipelago [1] and Rocketfuel [23] projects provide a set of widely-used topologies. They utilize `traceroute` from multiple vantage points and alias resolution techniques to construct router-level maps. Barford *et al.* [5] show that the utility of additional vantage points for `traceroute`-based topology discovery quickly decays. While their focus is on topological placement and indirect probing rather than subnet visibility and direct probe responsiveness, this decay in marginal utility is consistent with our findings.

Several other Internet measurement services also utilized multiple vantage points. The IDMaps project [15] explored the placement of mirror servers and instrumentation infrastructure for constructing distance (latency) maps. iPlane [17] predicts network path properties using a combination of methods, including isolating nodes to their BGP atoms [6], using traditional inference mechanisms, and collecting traffic information from instrumented network applications. Our techniques can be easily integrated with measurement services like iPlane [17] and the Scalable Sensing Service (S^3) [26].

Zhang *et al.* [28, 29] study the constancy of path properties over time, and distinguish the notions of mathematical, operational, and predictive constancies. Eriksson *et al.* [11] present an algorithm for estimating the route distance between Internet nodes in terms of hop counts using a small number of active measurements plus large collections of packet traces from passive captures, as well as BGP AS location information.

VIII. Conclusions and Future Work

In this paper, we demonstrate that direct and indirect probing differ in their visibility into network structures. We identify several reasons for this and quantify their prevalence. We then show that some areas of the network which are visible to indirect probing but not direct probing can be successfully explored by the addition of vantage points.

We present four methods for selecting vantage points for performing direct measurements that have good reachability into the network. We evaluate these methods on the Internet and find that leveraging route similarity performs substantially better than choosing vantage points at random.

We estimate that *five* vantage points selected by one of our methods would yield a total improvement in exposition of about 10% more subnets than probing from a single vantage point, and would match the performance of between 12 and 15 vantage points selected at random. Finally, we demonstrate that the returns of adding additional vantage points, even selected for effectiveness, diminishes rapidly after five.

Our future work plans include large-scale collection, validation, and analysis of topology maps using vantage points selected with the techniques in this paper, as well as techniques for selecting vantage points to be used for probing of specific destinations.

References

[1] Archipelago Measurement Infrastructure. http://www.caida.org/projects/ark/.

[2] The University of Oregon Route Views project. http://routeviews.org.

[3] Alexa Internet, Inc. Top 500 global sites. http://www.alexa.com/topsites/global, 2011.

[4] M. B. Akgün and M. H. Gunes. Link-level network topology generation. In *ICDCS Workshop on Simplifying Complex Networks for Practitioners*, June 2011.

[5] P. Barford, A. Bestavros, J. Byers, and M. Crovella. On the marginal utility of network topology measurements. In *ACM SIGCOMM Internet Measurement Workshop*, Nov. 2001.

[6] A. Broido and kc claffy. Analysis of RouteViews BGP data: policy atoms. In *Proc. of the Network Resource Data Management Workshop*, May 2001.

[7] R. Bush, O. Maennel, M. Roughan, and S. Uhlig. Internet optometry: assessing the broken glasses in internet reachability. In *Proc. of the ACM Internet Measurement Conference IMC*, November 2009.

[8] B. Chun, D. Culler, T. Roscoe, A. Bavier, L. Peterson, M. Wawrzoniak, and M. Bowman. Planetlab: An overlay testbed for broad-coverage services. *SIGCOMM CCR*, 33(3):3–12, 2003.

[9] I. Cunha, R. Teixeira, N. Feamster, and C. Diot. Measurement methods for fast and accurate blackhole identication with binary tomography. In *ACM IMC*, Chicago, IL, November 2009.

[10] B. Donnet and T. Friedman. Internet topology discovery: A survey. *IEEE Communications Surveys*, 9(4), 2007.

[11] B. Eriksson, P. Barford, and R. Nowak. Estimating hop distance between arbitrary host pairs. In *Proc. of IEEE INFOCOM*, March 2010.

[12] M. H. Gunes and K. Sarac. Analyzing router responsiveness to measurement probes. In *Proc. of PAM Conference*, April 2009.

[13] N. Hu and P. Steenkiste. Quantifying Internet end-to-end route similarity. In *Proc. of PAM Workshop*, pages 101–110, 2006.

[14] V. Jacobson. Traceroute. http://ftp.ee.lbl.gov/traceroute.tar.gz, 1989.

[15] S. Jamin, C. Jin, Y. Jin, D. Raz, Y. Shavitt, and L. Zhang. On the placement of Internet instrumentation. In *Proc. of the IEEE INFOCOM*, Tel Aviv, Israel, March 2000. http://www.ieee-infocom.org/2000/papers/586.ps.

[16] E. Katz-Bassett, H. Madhyastha, V. Adhikari, C. Scott, J. Sherr, P. van Wesep, A. Krishnamurthy, and T. Anderson. Reverse traceroute. In *Proc. of USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2010.

[17] H. V. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani. iPlane: An information plane for distributed services. In *Proc. of OSDI*, pages 367–380, Nov. 2006.

[18] P. Mérindol, B. Donnet, O. Bonaventure, and J. Pansiot. On the impact of layer-2 on node degree distribution. In *Proc. of ACM Internet Measurement Conference*, November 2010.

[19] J. Postel. Internet control message protocol. RFC 792, September 1981.

[20] L. Quan, J. Heidemann, and Y. Pradkin. Trinocular: Understanding internet reliability through adaptive probing. In *ACM SIGCOMM*, Hong Kong, August 2013.

[21] Y. Rekhter, R. Moscowitz, D. Karrenberg, G. de Groot, and E. Lear. Address allocation for private internets. RFC 1918, Feb. 1996.

[22] G. Siganos, M. Faloutsos, P. Faloutsos, and C. Faloutsos. Power-laws and the AS-level Internet topology. *IEEE/ACM Transactions on Networking*, 11(4):514–524, Aug 2003.

[23] N. Spring, R. Mahajan, D. Wetherall, and T. Anderson. Measuring ISP topologies with Rocketfuel. *IEEE/ACM Transactions on Networking (ToN)*, 12(1), February 2004.

[24] M. E. Tozal and K. Sarac. TraceNET: An Internet topology data collector. In *Proc. of ACM Internet Measurement Conference*, November 2010.

[25] R. van den Berg. tcpping. http://www.vdberg.org/∼richard/tcpping.html.

[26] P. Yalagandula, P. Sharma, S. Banerjee, S. Basu, and S.-J. Lee. s^3: A scalable sensing service for monitoring large networked systems. In *Proc. of the ACM SIGCOMM Workshop on Internet Network Management (INM)*, September 2006.

[27] H. Yan, B. Say, B. Sheridan, D. Oko, C. Papadopolous, D. Pei, and D. Massey. IP reachability differences: Myths and realities. In *Proc. of the IEEE Global Internet Symposium*, April 2011.

[28] Y. Zhang, N. Duffield, V. Paxson, and S. Shenker. On the constancy of internet path properties. In *In Proc. of ACM SIGCOMM Internet Measurement Workshop*, 2001.

[29] Y. Zhang, V. Paxson, and S. Shenker. The stationarity of Internet path properties: Routing, loss, and throughput. ACIRI Technical report, May 2000. http://userweb.cs.utexas.edu/∼yzhang/papers/station-tr00.pdf.