Subnet Level Network Topology Mapping

M. Engin Tozal, *Student Member, IEEE,* Kamil Sarac, *Member, IEEE,*
Department of Computer Science, University of Texas at Dallas, TX 75080 U.S.A.
{engintozal, ksarac}@utdallas.edu

***Abstract*—Internet topology at the network layer consists of routers and subnets, i.e., point-to-point or multi-access connections. Network measurement studies have focused on router level maps and derived characteristics of routers such as mean degree, degree distribution, clustering coefficient and betweenness. Considering the fact that subnets are also important building blocks of the Internet topology, this paper introduces a complementary view of network topologies named subnet level maps. Subnet level network topology maps represent subnets as vertices and depict routers as links connecting the vertices/subnets. Additionally, we introduce a tool, called `exploreNET`, for subnet discovery. Although `ExploreNET` is based on the same principals as our recent work `traceNET` [24], it differs from `traceNET` in its utilization in various domains. Particularly, it allows us discover the underlying subnet level topology map of a network rather than the map dictated by routing dynamics. Finally, we present an evaluation of `exploreNET` by using it to discover and analyze various subnet characteristics including degree distribution, capacity distribution and utilization for six geographically disperse public Internet Service Providers (ISPs).**

I. Introduction

Many research efforts on discovering and analyzing topology maps of ISPs or the Internet have appeared during the last decade [22], [18], [10]. These maps allow us to make networking infrastructures more robust, reliable, and efficient; build representative models of the Internet; and improve scalability and performance of Internet services [23], [17], [4].

Existing network layer topology mapping efforts focus on *router level* maps by grouping discovered IP addresses into vertices and representing the subnets as simple links between vertices/routers. These maps are then studied to understand various characteristics of the routers, e.g., degree distribution, mean degree, betweenness, and clustering coefficient. Similar to routers, subnets are composite structures. A subnet holds a set of interfaces, owns a subnet mask, possesses an IP address range, and assumes an interconnection technology such as point-to-point or multi-access link. Hence, considering subnets as simple links in network topology mapping process diminishes the fidelity of the resulting maps.

In this study, we propose a complementary graph representation of the Internet at the network layer called *subnet level* maps. Subnet level maps depict subnets as vertices and consider routers as links connecting these subnets to each other (see Figure 1). Studying topological characteristics of subnet level maps, in addition to router level maps, would improve our understanding of topological features of ISP networks and help us develop better synthetic graphs representing the Internet. Moreover, subnet level maps provide support for application layer Internet services such as inspecting whether two paths share a common link in constructing link disjoint overlay network systems.

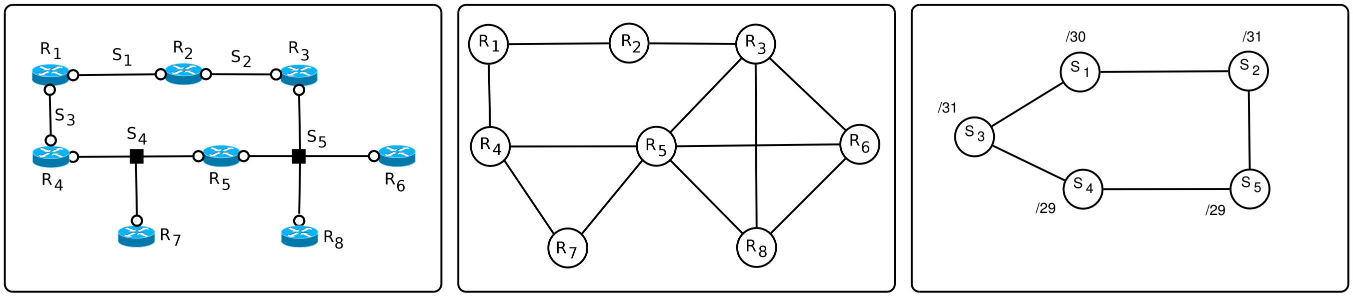
Recently, we introduced `traceNET` [24] a `traceroute`-like path tracing tool that collects the subnet information appearing on a path between two hosts in the Internet. Although path tracing tools provide valuable information as a network debugging and path analysis tools, they are insufficient when it comes to constructing representative network topologies. Most of the network topology mapping studies use path tracing from k vantage points toward m destinations where $k \ll m$ for collecting raw data and then process the data for building the maps. However, factors such as AS relationship policies, hot-potato routing, and internal routing preferences within an AS cause some sub-paths to be observed frequently while missing some other paths [22], [11]. At the extreme, path tracing customarily fails to discover backup links. Topology maps based on path tracing reflect *routing level* topologies, i.e., topologies dictated by the routing dynamics, rather than the underlying network topology. Consequently, path tracing induces restricted coverage and limited representation in building network layer topology maps [12], [1].

Console Output 1 Sample `exploreNET` session

```
# sudo ./xnet -d 24.173.8.28
Network Number : [Network IP Address - Hop Distance List]
-------------- :  -------------------------------------
24.173.8.24/29 : [24.173.8.26 - 2, 24.173.8.25 - 3,
                  24.173.8.29 - 3, 24.173.8.28 - 3]
```

In this paper, we propose an alternative way to construct subnet level network topologies for increasing coverage and representativeness. Instead of using a path tracing tool such as `traceNET`, we devise, `exploreNET`, a standalone network layer subnet discovery tool which is based on similar principles as with `traceNET`. Given a target IP address t as input, `exploreNET` uses active probes to discover the subnet S that contains t along with all other alive IP addresses on S. Additionally, it annotates S with its observable subnet mask. Console Output 1 gives a sample `exploreNET` execution to the destination IP address 24.173.8.28. In the output, `exploreNET` discovers a $/29$ subnet hosting the destination IP address along with the other alive IP addresses within the subnet. By providing the list of alive IP addresses of an ISP network as input to `exploreNET`, we can discover all the subnets utilized in the ISP from a single vantage point. Note that similar to other probe based network discovery tools, `exploreNET` cannot obtain a subnet in case its interfaces remain silent to probe packets or the border routers of an ISP drop probe packets or the corresponding response packets.

Although `exploreNET` shares similar design principles as with `traceNET`, it deviates from `traceNET` particularly in its utilization. First of all, while `traceNET` is appropriate for path analysis and debugging, `exploreNET` is a better option in studying standalone subnets. Secondly, a single vantage point is enough for `exploreNET` to collect all observable subnets within a target network domain whereas `traceNET` needs to be run from many vantage points to maximize its coverage. Thirdly, `exploreNET` could be well integrated into



(a) Example Internet Topology

(b) Router Level Topology Graph

(c) Subnet Level Topology Graph

Fig. 1: A network layer topology map (left) is represented as a router graph (center) and a subnet graph (right).

other network analysis tools due to its minimalist design. To illustrate, one can implement a `reverse-traceNET` tool by providing the IP addresses revealed on the reverse path from a destination to a source via `reverse-traceroute` [5]. Finally, `exploreNET` could be used to randomly sample subnets across the entire Internet to derive accurate statistics about the subnet related characteristics of the global Internet infrastructure at the network layer. The subnet statistics conforming to the real Internet could be used to generate synthetic networks for testing new protocols and algorithms before their deployment on the Internet.

In this paper, we present the internals of `exploreNET` and evaluate its completeness and accuracy rates against a ground truth set from the public Internet. Our evaluations demonstrate that `exploreNET` achieves 85% completeness and 93% accuracy. Next, we use it to discover subnet information for six ISPs including PCCW Global, nLayer, France Telecom, Telecom Italia Sparkle, Interroute, and MZIMA operating at different regions of the world and study the subnet level maps to identify common and discrete subnet characteristics that appear among these ISPs. Our experimental results show that 87% of the subnets we found are point-to-point links (/30 and /31). However, these point-to-point links accommodate only 23% of subnetized IP addresses, i.e., IP addresses that are successfully put into a subnet by `exploreNET`, while the rest of the IP addresses are hosted by multi-access links of various sizes. We also show that nLayer and France Telecom are the two ISP networks whose IP address space is highly utilized, i.e., at rates of 93% and 92%, respectively. Finally, our complete subnet discovery process over six ISP networks consists of many small and a few very large subnets. Yet, we showed that this pattern does not fit to power law distribution.

The rest of the paper is organized as follows. The next section presents the related work. Section III details the internals of `exploreNET` and demonstrates its accuracy and completeness. In Section IV we collect subnet level maps of six public ISPs and study their subnet level characteristics. Finally, Section V concludes the paper.

II. Related Work

Many successful tools and approaches have been suggested to derive a complete and accurate topology of the Internet at IP, router, and AS levels. Most of these works have been deployed for a long time and continue to collect and/or process Internet topology data [14], [10], [13], [25].

Siamwalla et al. introduced a set of algorithms for discovering IP level maps [20]. These algorithms utilize SNMP, ping, traceroute, and DNS info to collect in-use IP addresses in the Internet. Following studies not only seek for methods to penetrate into the deeps of the Internet but also focused on processing the data and build router and AS level maps.

DIMES [18] is a distributed route tracing and ping tool trying to reveal hidden parts of the Internet by using personal computers as vantage points. Rocketfuel [22] aims to reveal the router level map of a single AS by carefully selecting the sources and the destinations to include the target AS network on the path traces. DisCarte [19] uses logic programming to process IP record route option enabled traceroute data for constructing router level Internet topology maps.

AS level topology mapping uses various sources of information including BGP routing tables, traceroute, and Internet Registry databases for building a higher level map of the Internet [7], [2], [8].

Most of the studies on deriving various conclusions about the characteristics of the Internet used data collected by path tracing [6], [21]. Later, researchers argued about the validity of those claims by pointing out several limitations [12], [1].

`ExploreNET`, the topology discovery tool presented in this paper, is designed to discover individual subnets at the network layer whereas our previous tool `traceNET` [24] collects subnets appearing on a path between two hosts. Subnet level topology mapping, introduced in this study, nicely complements the existing schemes in discovering a more complete picture of the Internet topology at the network layer. We discover subnet level maps of the underlying genuine network structure via `exploreNET` rather than the limited network structure dictated by the routing dynamics via `traceNET`. This approach allows us to derive representative statistics of subnets in the Internet. To the best of our knowledge this is the first study introducing subnet level Internet topology mapping concept and presenting a tool for building such maps while decoupling the revealed map from the routing.

III. Network Layer Subnet Discovery

In this section, we present `exploreNET` and evaluate its accuracy in the public Internet. A subnet is a logically visible sub-section of a single Internet Protocol network (RFC 950) where the connected router (or end system) interfaces can directly communicate with each other at the network layer. However, from network layer perspective a subnet is independent from any configuration below layer-3 and it could be an Ethernet network, a virtual network established through MPLS tunnels, or an ATM cloud. Typically, a subnet is assigned a subnet (or a network) number that represents a range of IP addresses for assignment to the connected router interfaces on the subnet. Subnet discovery is defined as the process of bringing all in-use IP addresses of a subnet to light and annotating the subnet with its observed IP address space (i.e., subnet mask).

ExploreNET is an extension to our closely related tool traceNET [24]. TraceNET is designed to collect subnet-level info on an end-to-end routing path between two hosts. On the other hand, our goal in this study is to build an independent tool which discovers the subnet accommodating a given IP address. In simple terms, given a target IP address t, exploreNET grows hypothetical subnets encompassing t starting from $/31$ prefix length. For each IP address within the hypothetical subnet it sends probe packets to identify if the IP address is alive and checks whether the IP address is located within the subnet boundary. The subnet growing process continues until it encounters with an IP address that is not located within the boundary of the current hypothetical subnet. In that case exploreNET stops and returns the last valid subnet along with its alive IP addresses.

A. *ExploreNET Foundations*

In this part we explain foundations and assumptions on which we build our subnet discovery algorithm. In the next part we present the subnet discovery algorithm in detail.

A subnet S is a set consisting of a number of interfaces. From a network layer perspective, an interface l has an associated IP address and a hop distance from a particular vantage point v. The hop distance is subject to change over time, however, our experimental results show that it mostly remains stable during subnet discovery time which is on the order of a few seconds. We use l^{ip} to refer to the IP address of l and l^h_v to refer to the hop distance of l from v. Whenever the vantage point is clear in a context, we drop v and denote the hop distance by l^h. Degree of a subnet, S^d, is the number of interfaces accommodated by S and prefix length of a subnet, S^p, is the number of leftmost bits that are common to all IP addresses on S.

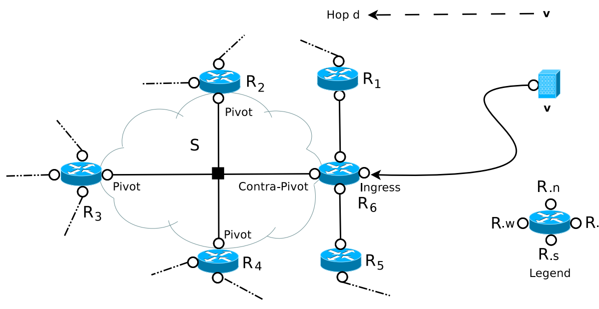


Fig. 2: A subnet S of size four located at hop distance d from vantage point v

Figure 2 shows a subnet S located at hop distance d w.r.t. the vantage point v. In the Figure, ovals and small circles represent routers and interfaces hosted by the routers, respectively. For the sake of clarity we refer to an interface of a router by its position on the router (n)orth, (w)est, (s)outh, and (e)ast as shown in the legend.

Assuming there is no path fluctuations caused by routing updates or load balancing, *ingress router* of a subnet S, w.r.t. a vantage point v, is the router that packets originated from v and destined to any interface on S are delivered through during a period of routing update. In Figure 2, R_6 is the ingress of S and packets from v destined to $R_2.s \in S$ or $R_3.e \in S$ enter S through R_6. Note that ingress router of a subnet does not get affected from intermediate path fluctuations as long as the fluctuated route converges at or before the ingress router.

Pivot interface of a subnet S is any interface on S that is not located on the ingress router of S w.r.t. a vantage point v. The interface located on the ingress router of a subnet is called *contra-pivot interface*. In Figure 2 interfaces $\{R_2.s, R_3.e, R_4.n\}$ are pivots and $R_6.w$ is the contra-pivot interface. Note that, assuming a stable ingress router to a subnet of degree m, there are $m-1$ pivot interfaces and one contra-pivot interface. *Unit subnet diameter* implies that two interfaces on the same subnet are located at most one hop distance apart w.r.t. a vantage point. In Figure 2, interfaces $\{R_2.s, R_3.e, R_4.n, R_6.w\} \in S$ are at most one hop apart from each other w.r.t. v.

Subnet exploration is carried out by forming a *temporary subnet* ($\bar{S}$) including a pivot interface and applying the tests defined in Section III-B to each and every IP address that can possibly be a member of the temporary subnet. Temporary subnets start from $/31$ prefix and as long as IP addresses of the temporary subnet pass from all the tests, the temporary subnet is grown by one level (i.e., grown from a prefix p to a prefix $p-1$ subnet). In case an IP address of a temporary subnet fails one of the tests, the algorithm shrinks one prefix level and stops (i.e., from prefix p to prefix $p+1$). At the end, all IP addresses that are alive and within the boundaries of the last temporary subnet prefix constitutes the subnet hosting the pivot interface.

Assume that we run exploreNET at a vantage point v to discover a subnet S that hosts a target IP address t. Initially, exploreNET needs to (i) determine the hop distance to t (i.e. t^h) and (ii) designate a pivot interface l that is on the same subnet with t. Determining t^h (distance to t) could easily be accomplished by sending ICMP probes to t with increasing and decreasing TTL values until its exact distance is found. This can also be achieved by sending one UDP probe and using the TTL field of the piggy-backed probe packet in the ICMP response message from t. Any two IP addresses that have left most 31 bits in common are called *mate-31* of each other. Given that i^{ip} and j^{ip} are two alive IP addresses and mate-31 of each other, then $i \in S \iff j \in S$. A similar but weaker definition could be made for *mate-30* relationship between two IP addresses. Designating a pivot interface, l, is done by probing mate-31 of t with $TTL = t^h$. If the response is an ICMP TTL_EXCEEDED, then t is the contra-pivot interface in S and its mate-31 is a pivot interface. On the other hand, if the response is an ICMP ECHO_REPLY then t is definitely a pivot interface. The reason behind this rule is that two IP addresses that are mate-31 to each other are most likely to be on the same subnet and their distance from a vantage point differs at most by one hop. In case mate-31 of t is unresponsive, we try mate-30 of t. Then, we send an indirect probe to the pivot interface, l, with $TTL = l^h - 1$ and use the source IP address field of the response message as an alias for ingress router. This alias to the ingress router is called *ingress interface*.

B. *ExploreNET Algorithm*

ExploreNET algorithm consists of a set of standalone tests that detect the boundaries of a subnet. In the following, we first elaborate on each test and its purpose and then present the algorithm.

The tests that we employ to determine the boundaries of a subnet S are based on the assumptions such as (i) under a stable path hop distances of the interfaces of a subnet differ at most by one unit w.r.t. a vantage point; (ii) IP addresses assigned to the interfaces of a subnet share a common subnet mask (prefix); (iii) two alive IP addresses that are mate-31 of each other are hosted by the same subnet; and (iv) packets destined to different interfaces of a subnet from a particular vantage point are most likely to enter into the subnet through the ingress router. Note that, one cannot expect that these assumptions always hold, however, our evaluations on public Internet ground truth data set shows that they work most of the time. In case, any of these heuristics does not hold, `exploreNET` terminates prematuraley and returns an underestimated subnet.

Given that l is the designated pivot interface and temporary subnet $\bar{S}$ is formed around l, let IP address i be in the IP address space of $\bar{S}$.

(i) Scope Delimitation Test is the process of conforming that i is located at hop distance l^h or $l^h - 1$. The test is carried out with two probes. If i is a pivot interface, an ICMP probe with $TTL = l^h$ should return an ICMP ECHO_REPLY and another probe with $TTL = l^h - 1$ should return an ICMP TTL_EXCEEDED. Additionally, the source address of the second probe must be the same with the alias of the ingress router. If i is a contra-pivot interface, both probes should result in ICMP ECHO_REPLY messages. If we do not get any response for the first probe than it is an indication that the IP address i is either not in use or not responsive. Then, we move to the next IP address in $\bar{S}$. If this test fails, we stop and shrink the temporary subnet $\bar{S}$ by one level.

Note that, scope delimitation test is not a strong test by itself because it is prone to various false positive interfaces depending on the configuration of a subnet and its surrounding subnets. We have categorized these false positive interfaces into three groups: far-fringe interfaces, close-fringe interfaces, and ingress-fringe interfaces. Figure 3 highlights each fringe interface category for the subnet introduced in Figure 2. None of the fringe interfaces belongs to the subnet being discovered. Ingress-fringe interfaces are the ones that are hosted by the ingress router. Far-fringe interfaces are hosted by routers that are one hop distant from the ingress router but are not accommodated by any subnet that the ingress router has direct access. Similarly, close-fringe interfaces are hosted by routers that are one hop distant from the ingress router but are accommodated by a subnet that the ingress router has direct access.

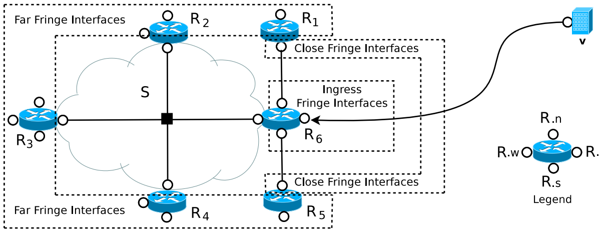


Fig. 3: Fringe interfaces of the subnet S presented in Figure 2

(ii) Non Far-Fringe Interface Detection Test is used to detect whether i is a far-fringe interface or not. It employs a single ICMP probe destined to the mate-31 address of i with $TTL = l^h$. Acquiring an ICMP TTL_EXCEEDED as response indicates that i does not belong to the subnet being discovered and it is a far-fringe interface. In case mate-31 of i is not responsive, we repeat the test with mate-30 of i. If an IP address fails from this test, the subnet growing process stops and $\bar{S}$ gets shrunk one level. In Figure 3, if mate-31 of $R_3.w$ is alive, we expect to get an ICMP TTL_EXCEEDED response to a probe destined to the mate-31 of $R_3.w$ with $TTL = l^h$.

(iii) Non Ingress-Fringe Interface Detection Test is used to detect whether i is an ingress-fringe interface or not. Ingress-fringe interfaces behave as if they are contra-pivot interfaces. During the subnet exploration we expect a single ingress router, hence, there should be a single contra-pivot interface of a subnet. Note that, we do not need any extra probes here. If Scope Delimitation Test catches another contra-pivot interface, we just stop and shrink the subnet $\bar{S}$ by one more level. Moreover, since we are expanding the temporary subnets around a pivot interface, the real contra-pivot interface will be encountered before the false positive ingress fringe interfaces. In Figure 3, all interfaces of R_6 except $R_6.w$ belong to the subnets other than the one being discovered and they are ingress-fringe interfaces.

(iv) Non Close-Fringe Interface Detection Test is used to detect whether i is a close-fringe interface or not. It is applied only to pivot interface candidates. It simply says that if mate-31 of a pivot interface is not the contra pivot interface, then ICMP probing the mate-31 address should not result in an ICMP ECHO_REPLY. If it does, mate-31 of i is a second contra-pivot interface and both i and its mate-31 are not part of the subnet S. In case mate-31 of i is not responsive, we repeat the test with mate-30 of i. As a reaction, the algorithm stops and shrinks $\bar{S}$ one more level.

Algorithm 1 EXPLORENET

```
Input: $t$ /*A target IP address*/
Output: $S$ /*Subnet $S$ along with all alive IP addresses and its observed subnet prefix*/
 1 $t^h \leftarrow$ find hop distance to t
 2 $l \leftarrow$ designate a pivot interface
 3 for $p \leftarrow 31$ to 0 do
 4     $\bar{S} \leftarrow$ form temporary subnet containing $l$ with prefix $p$
 5     for each $i^{ip} \in \bar{S}$ do
 6         if $i^{ip}$ is not tested before then
 7             if $i^{ip}$ passes Scope Delimitation Test then
 8                 if $i^{ip}$ fails Non Far-Fringe Interface Detection Test OR
                   $i^{ip}$ fails Non Ingress-Fringe Interface Detection Test OR
                   $i^{ip}$ fails Non Close-Fringe Interface Detection Test OR
                   then
 9                     Shrink $\bar{S}$ by one level and return $S \leftarrow \bar{S}$ with its alive IP addresses
10                 end if
11             else
12                 Shrink $\bar{S}$ by one level and return $S \leftarrow \bar{S}$ with its alive IP addresses
13             end if
14         end if
15     end for
16 end for
```

Algorithm 1 explores the subnet accommodating the target IP address t which is given as input. The first two lines in the algorithm find the hop distance to t and designate a pivot interface l as explained above. The outer-loop at lines 3-4 forms temporary subnets $\bar{S}$ starting from $/31$ around the pivot interface and the inner loop at lines 5-15 applies scope delimitation, non far-fringe, non ingress-fringe, and non close fringe tests to each IP address $i^{ip} \in \bar{S}$. If i^{ip} passes from all tests it would be an alive member of the final subnet S. On the other hand, in case of failure from tests the temporary subnet gets shrunk by one level, e.g., from $/27$ to $/28$, and the algorithm reaches termination by returning the final subnet S at line 9 or 12. Observed subnet mask (prefix length) of a subnet is the smallest size subnet mask encompassing all IP addresses of the subnet. It may or may not be actual, that is, given that a network administrator has allocated a $/29$ address space to a subnet but utilized only the first two IP addresses of the entire /29 address space, then exploreNET observes it as a /31 subnet.

C. ExploreNET Accuracy and Completeness

In this part, we consider the subnets obtained through mrinfo [9] as our ground truth set and use it to validate the accuracy and completeness rates of exploreNET.

Mrinfo is a multicast diagnostic tool which is used to query a router to learn the IP addresses of its multicast enabled interfaces along with the IP addresses of other multicast enabled interfaces on the same subnet. Recently, Pansiot et al. used mrinfo to infer partial topology information from several commercial networks [16]. The ground truth set consists of subnets that belong to and administered by various commercial ISPs scattered around the globe. Our findings show that exploreNET collects 85% (69%) of all the subnets reported by mrinfo excluding (including) the subnets whose interfaces do not respond to probe packets and its accuracy rate is 93%.

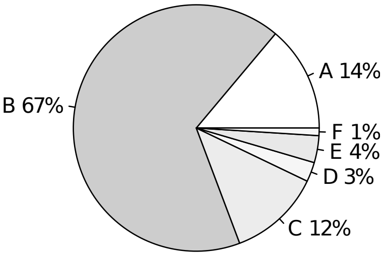


Fig. 4: Subnet taxonomy collected by exploreNET over mrinfo data

In this experiment we built our ground truth set, M, consisting of 5536 distinct subnets using the data provided by Pansiot [15] after clearing out 133 inconsistent subnets in the raw dataset. Then we picked an alive IP address l from each element of M and provide it to exploreNET as input. Figure 4 demonstrates the results obtained by exploreNET categorized into different sets labeled A thru F. In the figure each set is associated with its rounded percentage value w.r.t. the whole dataset. A denotes the set of mrinfo reported subnets that are completely unresponsive, that is, none of the IP addresses of the subnets in A responded to direct ICMP probes. Since the IP addresses of subnets in A are silent to probes there is no other way to learn about the existence of these subnets via active probing and there are 768 such subnets, i.e., $|A| = 768$. Among $|M - A| = 4768$ subnets, exploreNET successfully constructed 3702 subnets with all its IP addresses exactly as reported by mrinfo. In the figure this set is indicated by B. On the other hand, exploreNET could not grow 673 subnets, C, because it could not find an appropriate pivot interface. Finally, 393 subnets collected by exploreNET were different from the ones reported by mrinfo. Analyzing these 393 misinferred subnets further, revealed that 142 of these exploreNET collected subnets, denoted by set D, subsume their corresponding ones that are reported by mrinfo in terms of the set of IP addresses. Note that mrinfo accounts for the IP addresses of multicast enabled interfaces, hence, having subnets larger than the reported ones is quite likely. 196 of the remaining 251 misinferred subnets are the ones that we could not obtain a response from all of their reported IP addresses, i.e., partially unresponsive, and we use symbol E to represent this set. Lastly, the remaining 55 subnets, denoted by set F, have both unresponsive IP addresses that were not captured by exploreNET and responsive IP addresses that were not reported by mrinfo.

Completeness rate of exploreNET can be defined in two ways. In the first case, we account for the unresponsive subnets in our measurement and define completeness rate as the percentage of successfully obtained subnets w.r.t. the whole dataset, i.e., $|B{\cup}D|/|M| = 69\%$. In the second case, we define it as the percentage of successfully obtained subnets w.r.t. all subnets that are responsive, i.e., $|B \cup D|/|B \cup C \cup D| = 85\%$. Note that while measuring the completeness rate in the second case, we disregard subnets in sets A, E and F because they are completely or partially unresponsive to ICMP probes. On the other hand, we account for the set C which denotes the subnets that exploreNET could not designate a proper pivot interface. Designating a pivot interface is a feature of exploreNET that we can penalize it for. However, exploreNET does not misinfer the subnets in C but reports them as un-inferred (/32) subnets. Therefore, we can define accuracy rate metric as $|B \cup D|/|B \cup D \cup E \cup F| = 93\%$.

IV. Experimental Results

In this section, we use exploreNET to discover subnet level topologies of six geographically disperse ISP networks including PCCW Global (ISP-1), nLayer (ISP-2), France Telecom (ISP-3), Telecom Italia Sparkle (ISP-4), Interroute (ISP-5), and MZIMA (ISP-6) and use these topologies to analyze their subnet characteristics. First, we identify the IP address space for each ISP. Then, using an AS relationship dataset provided by CAIDA[1], we remove the ranges of IP addresses that are assigned to their customer domains. This pre-processing step enables us to focus on the backbone ISP networks excluding the topology information of their customer domains which are managed and operated by others. Next, we utilize active probing to identify alive IP addresses forming our observable IP address set as given in Table I. The numbers in the table show observable IP addresses in the backbone of the above ISPs excluding their customer networks.

TABLE I: Alive IP address distribution for target ISPs

ISP-1	ISP-2	ISP-3	ISP-4	ISP-5	ISP-6	Σ
45,018	54,636	17,170	8,380	21,209	16,453	162,866

In the rest of this section, first we analyze subnet degree and subnet prefix length distribution for each ISP. Then, we study IP address space utilization pattern in each target ISP. Finally, we check to see if the aggregate subnet degree and prefix length distributions conform to power-law.

A. Subnet Degree Distribution

Degree of a subnet refers to the number of interfaces (or alive IP addresses) accommodated by the subnet. In this part we take a close look at the degree distributions of six ISPs and identify the common and discrete subnetting practices among these ISPs. In short, most of the subnets are of degree two which is also the median degree. Therefore, the degree distributions are highly skewed. On the other hand, two ISPs host a small number of very large degree subnets consisting of thousands of IP addresses which belong to Akamai Technologies.

[1] http://www.caida.org/data/

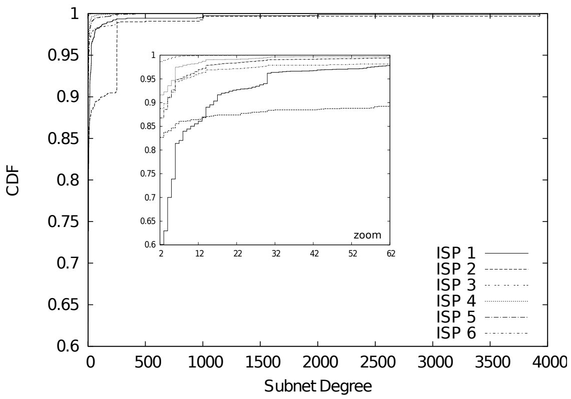


Fig. 5: Degree Distribution CDF for public ISPs

Figure 5 shows the subnet degree cumulative distribution functions (CDFs) for each of the six ISPs. Due to scaling issues we zoomed the portion of the figure where at least 90% of the subnets is captured for each ISP. The zoomed portion is inlined in Figure 5. An immediate observation in the CDFs is that the subnets having degree two comprises the majority of the subnets. The CDF curve belonging to ISP-1 starts at 60% at degree two and the one belonging to ISP-3 starts at 98% while the rest take values in between. This fact suggests that the median degree (50th-percentile) is two for all ISPs and their degree distributions are highly skewed.

TABLE II: Subnet Degree Statistics

	ISP-1	ISP-2	ISP-3	ISP-4	ISP-5	ISP-6	Σ
Max	3931	3933	109	245	429	254	3933
Min	2	2	2	2	2	2	2
Mean	18.23	44.90	2.06	2.84	3.99	6.74	7.36
Median	2	2	2	2	2	2	2
Std	166.19	246.75	1.34	7.82	16.87	30.61	82.87

Table II presents the maximum, minimum, mean, and median degree for each ISP as well as the standard deviation. Among these six ISPs, PCCW Global (ISP-1) and nLayer (ISP-2) have the highest mean degree values which is due to 10 subnets that have degrees more than 2000. On the other hand, the number of very large-sized subnets are not that many compared to small-sized subnets in ISP-1 and ISP-2 which explains the high standard deviations in the subnet degrees of these two ISPs. 98% of the subnets in France Telecom (ISP-3) network have degree two and there is only one subnet in this network with degree greater than 25. Hence, ISP-3's mean and median degrees are very close to each other and the small standard deviation suggests a more stable degree distribution in the network.

Although these 10 very large subnets seem to be uncommon, exploreNET confirmed for each subnet that probe packets destined to each IP address within the subnet pass through the same ingress router and all IP addresses are located at the same hop distance except the contra-pivot which is located one hop closer to the vantage point. Besides, mate-31 (mate-30) addresses of these IP addresses are also within the subnet boundaries and all passed the tests defined in Section III.

A close examination of a randomly selected 1000 IP addresses from each of these large subnets via DNS name resolution queries revealed the fact that all these subnets belong to Akamai Technologies, an online content distribution service provider with a global presence in the Internet. The reason that these hosts do appear in the ISPs' network rather than Akamai network is Akamai deploys its content servers within ISPs' networks [23]. Moreover, the DNS names of all IP addresses within a subnet share the same prefix as `a72` in `a72-247-183-101.deploy.akamaitechnologies.com`. These large subnets are part of Akamai data centers which might be realized either at the data link layer where the interfaces communicate through bridges or at the network layer where the interfaces communicate through tunnels.

B. Prefix Length Analysis

Subnet prefix length can be used as a quantitative measure denoting the capacity of a subnet. ExploreNET not only collects the IP addresses sharing the same subnet but also labels the subnets with their observed subnet masks. In this experiment, we analyze the subnet prefix length distribution patterns along with their summary statistics of our target ISPs. Briefly, our results show that 87% of subnets are point-to-point links yet they accommodate only 23% of successfully subnetized IP addresses. Additionally, France Telecom (ISP-3) and Telecom Italia Sparkle (ISP-4) prefer $/31$ subnets over $/30$ subnets in forming point-to-point links whereas for the other ISPs we do not observe such a clear trend.

TABLE III: Subnet prefix length distributions for ISPs

	ISP-1	ISP-2	ISP-3	ISP-4	ISP-5	ISP-6	Σ
/20	3	4	0	0	0	0	**7**
/21	3	0	0	0	0	0	**3**
/22	7	7	0	0	0	0	**14**
/23	3	2	0	1	6	0	**12**
/24	24	110	1	2	14	36	**187**
/25	25	8	0	7	6	7	**53**
/26	123	14	0	11	28	10	**186**
/27	152	17	7	28	78	34	**316**
/28	262	26	29	82	215	70	**684**
/29	440	48	115	131	419	136	**1289**
/30	899	418	316	177	2179	535	**4524**
/31	429	552	7394	2378	1567	1494	**13814**
Σ	**2370**	**1206**	**7862**	**2817**	**4512**	**2322**	**21089**

Table III shows the prefix length distributions for the target ISPs. Each cell in the table represents the number of subnets of a certain prefix length collected in a particular ISP network. Additionally, exploreNET returned 7557 $/32$ subnets. These are single IP addresses for which exploreNET could not grow a subnet because probing possible member IP addresses of the subnet did not return any response.

Table III shows that 87% of the subnets in the ISPs' backbones are point-to-point links consisting of $/31$ and $/30$ subnets. Nevertheless, accounting for the large number of IP addresses that multi-access LANs can host, subnets with smaller prefix (larger capacity) constitute a significant part of the backbone of these ISP networks. $/31$ subnetting (RFC 3021) for point-to-point links has been introduced several years after standard subnetting procedure (RFCs 950, 1878) in order to improve IP address utilization. However, examining prefix length distributions demonstrates that $/31$ subnetting is not intensely dominant in point-to-point links except for France Telecom (ISP-3) and Telecom Italia Sparkle (ISP-4) among our six target ISPs.

One interesting pattern is observed when we analyze the prefix length trends of the ISPs. Specifically, as the prefix lengths decrease, the number of observed subnets decrease faster. However, this trend breaks for many of the ISPs at $/24$. We believe the reason behind this is that $/24$ prefix length is a popular choice for constructing subnets compared to $/25$ or $/23$ and exploring periphery of the Internet might reveal much more $/24$ subnets.

Another interesting point in our analysis comes out when we read Tables I and III together. In Table I, nLayer (ISP-2) has 54,636 alive IP addresses while France Telecom (ISP-3) has 17,170. On the other hand, in Table III nLayer has 1,206 distinct subnets while France Telecom has 7,862. Analyzing the prefix length distributions of both ISPs in Table III reveals the fact that nLayer has large subnets accommodating many IP addresses while France Telecom has many small subnets accommodating less IP addresses.

TABLE IV: Mean and standard deviation of prefix lengths

	ISP-1	ISP-2	ISP-3	ISP-4	ISP-5	ISP-6	Σ
Mean	29.20	29.61	30.91	30.67	30.04	30.35	30.36
Std	1.64	2.23	0.38	0.89	1.04	1.23	1.21

Finally, Table IV show that the average prefix length among these ISPs is 30.36 which suggests that the majority of subnets are point-to-point links. Relatively large standard deviation of nLayer (ISP-2) suggests the variability in utilization of subnet prefix lengths hence, subnet sizes, is high whereas France Telecom (ISP-3) prefers a more stable subnet deployment policy regarding the subnet sizes.

C. IP Address Space Utilization

In this section, we analyze IP address space utilization patterns of our target ISPs. `ExploreNET` annotates the subnets with their observed subnet masks while discovering their in-use IP addresses. Subnet mask (or prefix length), c_i, of a subnet, S_i indicates the IP address space (capacity) of a subnet while degree, d_i, of the subnet indicates how many of IP addresses in the IP address space of the subnet have actually been utilized. Capacity, c_i, of a subnet, S_i, is defined as

$$c_i = \begin{cases} 2 & \textit{if } S_i \textit{ is a } /31 \textit{ subnet} \\ 2^{32-p} - 2 & \textit{if } S_i \textit{ is a } /p \textit{ subnet} \\ & \textit{such that } p \leq 30 \end{cases} \tag{1}$$

where p is the prefix length. Utilization rate of a subnet, S_i, is defined as the proportion of the degree of S_i to the capacity of S_i, i.e., $U_i = d_i/c_i$, except for $/30$ prefix. Utilization for subnets having $/30$ prefix is always 0.5 because the same IP network could have been assigned a $/31$ subnet number. The utilization rate, $\mathcal{U}$, of an entire ISP network is defined as

$$\mathcal{U} \quad = \quad \frac{\sum\limits_{\forall S_i} d_i}{\sum\limits_{\forall S_i} c_i}, \qquad \textit{such that } S_i \in ISP \tag{2}$$

Alternatively, internal IP address space waste for an ISP, $\mathcal{W}$, is defined as $\mathcal{W} = 1 - \mathcal{U}$. Note that, the internal IP address space waste is inevitable except for $/30$ subnets, e.g., constructing a subnet of size 150 requires allocating a $/24$ subnet with capacity 254; on the other hand, a $/30$ subnet could be divided into two $/31$ subnets. Our results show that nLayer (ISP-2) and France Telecom (ISP-3) have the least rate of IP address space waste while the aggregate waste is 20%.

Table V shows IP address space utilization of our target ISPs. In the table, each cell denotes the number of alive IP addresses discovered at a particular subnet prefix length (row) in a particular ISP network (column). Additionally, the marginal row and column labeled with $\mathcal{U}$ in the table show the IP address space utilization percentages against subnet prefix lengths and ISPs, respectively.

TABLE V: IP address space utilization of ISPs

	ISP-1	ISP-2	ISP-3	ISP-4	ISP-5	ISP-6	$\mathcal{U}$
/20	11790	15728	0	0	0	0	**96%**
/21	5939	0	0	0	0	0	**97%**
/22	6946	6969	0	0	0	0	**97%**
/23	923	785	0	197	2040	0	**64%**
/24	3803	26855	109	398	2547	8818	**90%**
/25	1610	632	0	503	397	564	**56%**
/26	3338	590	0	308	1144	426	**50%**
/27	2595	330	112	421	1351	641	**57%**
/28	1896	193	192	529	1661	596	**53%**
/29	1721	132	390	559	1402	553	**62%**
/30	1798	836	632	354	4358	1070	**50%**
/31	858	1104	14788	4756	3134	2988	**100%**
$\mathcal{U}$	**73%**	**93%**	**92%**	**74%**	**63%**	**84%**	**80%**

Analyzing the utilization column in Table V shows that very large subnets (e.g., $/20$, $/21$, and $/22$) that belong to Akamai Technologies are highly utilized. The column does not convey any significant pattern or figure except that $/31$ subnets are always completely utilized because a subnet must have at least two IP addresses and a $/31$ subnet cannot accommodate more than two IP addresses.

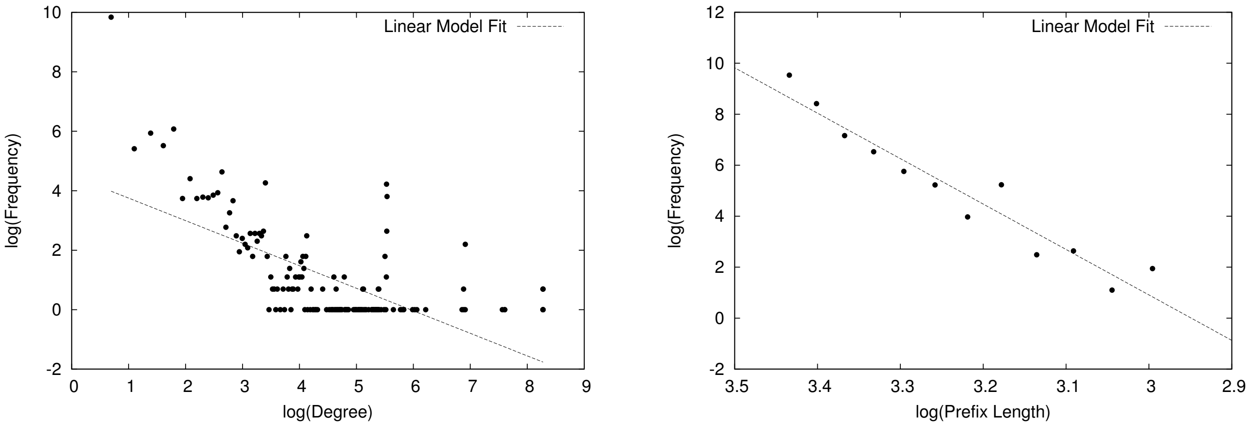
Utilization row in Table V presents that nLayer (ISP-2) and France Telecom (ISP-3) have the highest utilization rates while Interroute (ISP-5) has the lowest. Cross checking the prefix length distribution of Interroute (ISP-5) in Table III demonstrates the fact that high number of $/30$ subnets appearing in Interroute (ISP-5) is an important source of its low utilization rate. Indeed, excluding $/30$ subnets and re-calculating the utilization percentage for Interroute (ISP-5) resulted in an increase of 5 points.

Finally, alternative to the 87% significance of point-to-point links ($/30$ and $/31$) appearing in Table III, Table V shows that collectively these point-to-point links accommodate only 23% of the IP addresses that have been subnetized. In other words, multi-access LANs also form an important part of ISP networks by hosting 77% of subnetized IP addresses.

D. Quest for Power Law in Aggregate Distributions

In this section, we test whether aggregated prefix length and degree distributions of ISPs conform to power law [3]. Power law has been considered as the distribution model of various entities in the context of Internet topology measurements [21]. Power law indicates the existence of a few objects with very high frequency along with many objects with less frequency. A variable x is said to conform power law if its distribution is in the form of $p(x) \propto x^{-\alpha}$ where α is the scaling parameter [3].

Sections IV-A and IV-B demonstrate that most of the subnets in the target ISPs have small degree and capacity while the number of observed subnets decreases drastically as degree and capacity (prefix length) increases (decreases). This pattern suggests plausible power law relations in subnet degree and prefix length distributions. A necessary but not sufficient condition of power law relation is the linearity in log-log plot, i.e., $log(p(x)) \propto -\alpha log(x)$. Figures 6a and 6b demonstrate aggregate subnet degrees and prefix lengths against their frequencies in log-log scale. Additionally, the figure shows the linear regression function estimated using maximum likelihood estimation. Figures 6a and 6b visually articulate the large deviations of degree outliers such as 252, 253, 254, and



(a) Degree vs Frequency Log-Log Plot

(b) Prefix Length vs Frequency Log-Log Plot

Fig. 6: Prefix Length vs Frequency Plot in Increasing Subnet Size Order

1004 and prefix length outliers such as /31, /24, and /20 from the fitted line, respectively. Consequently, log-log plots are not linear and we can reject the existence of power law relations in subnet degree and prefix length distributions without conducting further statistical analysis.

V. Conclusions

In this paper, we have presented an active probe based tool, called `exploreNET`, to discover network layer subnet information and suggested several potential use of this information in Internet topology measurements and other application areas. Our evaluations show that `exploreNET` achieves 85% completeness and 93% accuracy rates on a ground truth data set in the public Internet.

Moreover, we use `exploreNET` to discover subnet information for six ISPs operating at different regions of the world. Our experimental results show that 87% of the subnets we found are point-to-point links (/30 and /31). However, these point-to-point links accommodate only 23% of subnetized IP addresses, i.e., IP addresses that are successfully put into a subnet by `exploreNET`, while the rest of the IP addresses are hosted by multi-access links of various sizes. We also show that nLayer and France Telecom are the two ISP networks whose IP address space is highly utilized, i.e., at rates of 93% and 92%, respectively. Finally, we showed that both degree and prefix distributions of subnets in these six ISPs do not conform to power law which is a common pattern occurring in complex systems.

Our future work in the area includes the use of `exploreNET` to build more representative network layer topology maps including both routers and subnets for several backbone domains and the use of the tool to conduct a statistical analysis of the subnet characteristics of the global Internet infrastructure via random sampling of subnets. Finally, an implementation of the tool is available at our project web site at `http://itom.utdallas.edu`.

References

[1] D. Achlioptas, A. Clauset, D. Kempe, and C. Moore. On the bias of traceroute sampling. In *ACM STOC*, Baltimore, MD, USA, May 2005.

[2] H. Chang, S. Jamin, and W. Willinger. Inferring AS-level Internet topology from router-level path traces. In *ITCom*, August 2001.

[3] A. Clauset, C. R. Shalizi, and M. E. J. Newman. *SIAM Review*, 51(4):661–703, 2009.

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

[5] E. Katz-Bassett, H. Madhyastha, V. Adhikari, C. Scott, J. Sherry, P. van Wesep, A. Krishnamurthy, T. Anderson. Reverse Traceroute. In *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, Sn Jose, CA, USA, April 2010.

[6] M. Faloutsos, P. Faloutsos, and C. Faloutsos. On power-law relationships of the internet topology. In *SIGCOMM '99: Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication*, volume 29, pages 251–262, New York, NY, USA, October 1999. ACM.

[7] L. Gao. On inferring autonomous system relationships in the internet. *IEEE/ACM Trans. Netw.*, 9(6):733–745, December 2001.

[8] B. Huffaker, A. Dhamdhere, M. Fomenkov, and Claffy. Toward Topology Dualism: Improving the Accuracy of AS Annotations for Routers. In *Proceedings of the 11th Passive and Active Measurement Conference (PAM 2010)*, Zurich, Switzerland, April 2010.

[9] V. Jacobson. Mrinfo. 1995. Available from http://cvsweb.netbsd.org/bsdweb.cgi/src/usr.sbin/mrinfo.

[10] D. M. K. Claffy, Tracie E. Monk. Internet Tomography. *Nature*, Jan 1999.

[11] S. Kim and K. Harfoush. Efficient estimation of more detailed Internet IP maps. In *IEEE ICC*, Glasgow, Scotland, Jun 2007.

[12] A. Lakhina, J. Byers, M. Crovella, and P. Xie. Sampling biases in IP topology measurements. In *IEEE INFOCOM*, San Francisco, CA, USA, Mar 2003.

[13] M. Luckie. *IPv6 Scamper*. WAND Network Research Group, 2005.

[14] H. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani. iPlane: An information plane for distributed services. In *OSDI*, Seattle, WA, USA, Nov 2006.

[15] P. Merindol, B. Donnet, J.J. Pansiot. On the Impact of Layer-2 on Node Degree Distribution. In *IMC Internet Measurement Conference*, Melbourne, Australia, Nov 2010.

[16] J.-J. Pansiot, P. Mérindol, B. Donnet, and O. Bonaventure. Extracting intra-domain topology from mrinfo probing. In *Proceedings of the 11th international conference on Passive and active measurement*, PAM'10, pages 81–90, 2010.

[17] R. Pastor-Satorras and A. Vespignani. *Evolution and Structure of the Internet*. Cambridge University Press, 2004.

[18] Y. Shavitt and E. Shir. DIMES: Distributed Internet measurements and simulations. Project page http://www.netdimes.org.

[19] R. Sherwood, A. Bender, and N. Spring. DisCarte: A disjunctive internet cartographer. In *ACM SIGCOMM*, Seattle, WA, USA, Aug 2008.

[20] R. Siamwalla, R. Sharma, and S. Keshav. Discovering internet topology. Technical report.

[21] 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.

[22] N. Spring, R. Mahajan, D. Wetherall, and T. Anderson. Measuring ISP topologies with Rocketfuel. *IEEE/ACM Transactions On Networking*, 12(1):2–16, Feb 2004.

[23] A.-J. Su, D. R. Choffnes, A. Kuzmanovic, and F. E. Bustamante. Drafting behind akamai (travelocity-based detouring). *SIGCOMM Comput. Commun. Rev.*, 36:435–446, August 2006.

[24] Tozal M. Engin, Sarac Kamil. TraceNET: An Internet Topology Data Collector. In *IMC Internet Measurement Conference*, Melbourne, Australia, Nov 2010.

[25] D. G. Waddington, F. Chang, R. Viswanathan, and B. Yao. Topology discovery for public ipv6 networks. *SIGCOMM Comput. Commun. Rev.*, 33:59–68, July 2003.