Investigating Interdomain Routing Policies in the Wild

Ruwaifa Anwar
Stony Brook University

Haseeb Niaz
Stony Brook University

David Choffnes
Northeastern University

Ítalo Cunha
Universidade Federal de Minas Gerais

Phillipa Gill
Stony Brook University

Ethan Katz-Bassett
University of Southern California

Abstract

Models of Internet routing are critical for studies of Internet security, reliability and evolution, which often rely on simulations of the Internet's routing system. Accurate models are difficult to build and suffer from a dearth of ground truth data, as ISPs often treat their connectivity and routing policies as trade secrets. In this environment, researchers rely on a number of simplifying assumptions and models proposed over a decade ago, which are widely criticized for their inability to capture routing policies employed in practice.

In this study we put Internet topologies and models under the microscope to understand where they fail to capture real routing behavior. We measure data plane paths from thousands of vantage points, located in eyeball networks around the globe, and find that between 14-35% of routing decisions are not explained by existing models. We then investigate these cases, and identify root causes such as selective prefix announcement, misclassification of undersea cables, and geographic constraints. Our work highlights the need for models that address such cases, and motivates the need for further investigation of evolving Internet connectivity.

1. INTRODUCTION

Research on existing and new protocols on the Internet is challenging because key aspects of the network topology is hidden from public view by interdomain routing protocols, and deploying new protocols at Internet scale requires convincing large numbers of autonomous networks to participate. As a result, networking researchers rely on assumptions, models, and simulations to evaluate new protocols [12, 24], network reliability [19, 34], and security [3, 15, 22].

Our existing models of interdomain routing [10], however, have important limitations. They are built and validated on the same incomplete topology datasets, typically routes observed via route monitors such as RouteViews and RIS. These vantage points expose a large fraction of paths from global research & education networks (GREN) and core networks, but they are incomplete in two keys ways. First, they expose few paths to and from eyeball and content networks. Second, they do not expose less preferred paths that would be used if the most preferred next-hop AS were not available. As a result, they do not capture partial peering, more complex routing policies based on traffic engineering, or load balancing and the rich peering mesh which exists near the edge of the network [31].

While limitations of our existing models are well known [25, 27, 31]–and are even being addressed in recent work [14]–we lack a solid understanding of how much these limitations impact our ability to accurately model the interdomain routing system. Recent work has attempted to address this issue by observing destination-based routing violations in control plane data [26] and by surveying a population of network operators about their policies [11], however, these approaches are limited in terms of scale and their ability to observe behavior at the network edge.

In this paper, we take a systematic approach to understanding how our models of routing policies hold in practice. To accomplish this, we leverage a combination of data-plane measurements covering the network edge ("eyeball networks") and control-plane experiments which allow us to directly measure relative preference of routing options. We create a methodology that takes into account numerous potential causes of violations to our assumptions including sibling ASes, complex AS relationships, prefix-specific routing policies, and the impact of geography. We use this methodology to investigate the prevalence of each of these sources of error in AS-level paths observed via measurements of the data and control planes.

With these measurements, we revisit generally held assumptions and models of Internet routing. Our goal is *not* to measure a complete Internet topology; rather, we seek to improve our understanding of routing decisions made by ASes when routing their traffic. Towards this goal we make the following observations for our measured paths:

- Hybrid and partial transit relationships (*e.g.*, those explored in [14]) contribute a surprisingly small amount to unexpected routing decisions.
- Per-prefix routing policies explain 10-20% of unexpected routing decisions, where an AS chooses a longer or more expensive path than our model predicts.
- We find that some large content providers like Akamai and Netflix are destinations for a large fraction (21% and 17%, respectively) of unexpected routing decisions.

- Routing decisions vary based on geography. We find paths that traverse multiple continents deviate from our models more, owing to undersea cable ASes which are not accounted for in our models of AS relationships, and a tendency for ASes to prefer non-international paths when endpoints are in the same country.

Our results highlight areas where more investigation would yield the largest payoff in terms of improving our accuracy when modeling AS relationships and routing policies. We also identify key areas, specifically investigating prefix-specific routing policies, where additional vantage points and looking glass servers could improve the fidelity of our AS topology data.

2. MODELING INTERDOMAIN ROUTING

The now standard model of routing policies was developed by Gao and Rexford [9, 10] based on seminal work by Griffin, Sheppard, and Wilfong [16] and Huston [17, 18]. In this model, ASes connect to each other based on business relationships: (1) customer-provider, where the customer pays the provider and (2) peer-to-peer, where the ASes engage in settlement-free peering and exchange traffic at no cost. This model gives the following view of local preferences and export policies, based on the economic considerations of ASes:

Local Preferences. An AS will prefer routes through a neighboring customer, then routes through a neighboring peer, and then routes through a provider.

Export Policy. A customer route may be exported to all neighboring ASes. A peer or provider route may only be exported to customers.

This model is sometimes augmented with the assumption that ASes only consider the next hop AS on the path when making their routing decisions. This simplifies analysis and makes debugging more tractable [19]. Simulation studies also often restrict path selection to the shortest among all paths satisfying Local Preference to induce unique routing decisions [12, 13].

While the above model and variations of it have been used in many studies (*e.g.*, [3, 12, 15, 20, 34]), it is well known that this model fails to capture many aspects of the interdomain routing system [25, 27, 31]. These aspects include AS relationships that vary based on the geographic region [14] or destination prefix, and traffic engineering via hot-potato routing or load balancing.

Prior work has used traceroute measurements and BGP data to address some of these issues (*e.g.*, [25, 27]); however, these measurements only offer a glimpse into ASes' routing preferences. Namely, they expose only the set of paths that are in use at the time of measurements. Further, these datasets have poor or no coverage of paths used by edge networks serving residential users [7]. On a smaller scale, network operators were surveyed about their routing policies to better understand how our models correspond to practice [11], but the scale and representativeness of a survey approach makes generalizing these observations infeasible.

3. METHODOLOGY

We aim to understand the gap between interdomain routing models and empirically observed behavior on the Internet. Our methodology combines two measurement techniques to gain better visibility into interdomain routing policies. First, we measure paths between edge networks and content providers to understand routing on paths that carry the bulk of the Internet's traffic [32]. Second, we perform BGP announcements to explore less preferred paths and directly measure relative preference among next-hop ASes.

3.1 Data-plane measurements

It is well known that a disproportionately large amount of Internet traffic originates from a few popular content providers [21, 32] towards large populations of end users. However, there is little empirical data about the paths this traffic takes [21]. We target our data plane measurements to cover these paths. Note that it is not our goal to explain routing decisions for the entire Internet. Rather, we focus on the more tractable task of measuring a subset of important Internet paths (those carrying most traffic) from a diverse set of vantage points, and putting those paths under the microscope to understand how and why they differ from predicted paths based on routing models.

Selecting content providers. We consider a list of the top applications from Sandvine [32] and top Web sites from Quantcast [29] and arrive at a list of 34 DNS names representing 14 large content providers.

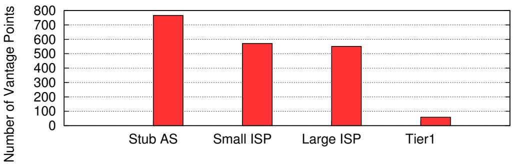


Figure 1: Distribution of the RIPE Atlas probes used in this study.

Vantage points (VPs). We leverage the RIPE Atlas platform which provides a large collection of probes located around the world for our traceroute measurements. RIPE Atlas has broad global coverage, but is known to have a disproportionate fraction of probes in Europe. To avoid a bias towards European ASes, we determine how many probes we would like to use and evenly divide the number of probes across all continents. We then start choosing probes from countries within each continent in a round robin manner focusing on distributing probes in different ASes within each country. We do this for each continent until we have allocated the target number of probes. Figure 1 summarizes the location of these probes in terms of AS type using the categorization method of Oliveira *et al.* [28]. The bulk of the probes are located near the network edge in stub and small ISP networks.

To measure paths to content providers, each RIPE Atlas node performs a DNS lookup for each of the 34 content DNS names, and then performs a traceroute to the resolved IP. In our experiments we use 1,998 RIPE Atlas probes,[1] located in 633 ASes, distributed according to our sampling methodology. Combined, these probes perform 28,051 traceroutes to 218 destination ASes. The number of destination ASes is large relative the number of content providers because large numbers of content servers are hosted outside the provider's network (*e.g.*, inside ISPs).

From traceroutes to routing decisions. We convert the traceroute-based IP-level paths into AS paths using the method described by Chen et al. [7]. Since interdomain routing is destination based, we can observe routing decisions for all ASes along the path to a given destination. We thus observe routing decisions for a total of 746 ASes.

3.2 Control-plane measurements

Data-plane measurements observe only the most preferred route for an AS toward a destination. We use PEERING [33] to expose alternate, less preferred routes and to attempt to reverse engineer BGP decisions.

PEERING operates an ASN and owns IP address space that we can announce via several upstream providers. PEERING allows us to manipulate BGP announcements of its IP prefixes and observe how ASes on the path react. We used PEERING to announce prefixes using providers at six US universities (GaTech, Clemson, Southern California, Northeastern, Stony Brook, and Cornell) and one university in Brazil. We change announcements at most once per 90 minutes to allow for route convergence and avoid route flap dampening. We use traceroutes from PlanetLab and RIPE Atlas, as well as BGP feeds from RouteViews and RIPE RIS, to monitor paths toward PEERING prefixes.

Discovering alternate routes. We start announcing an IP prefix from all PEERING locations in an 'anycast' announcement. At each round, we observe the preferred route at a target AS T and the next-hop neighbor N that T is using to route toward our prefix. We then poison N, *i.e.*, add N's AS number to the path [4, 8], to trigger BGP loop prevention at N and cause N to no longer have a path to our prefix (and stop announcing a route to T). This forces T to choose a different route, through a different neighbor N'. We repeat this process in consecutive rounds, poisoning the newly-discovered neighbor, to identify all neighbors and routes T can use toward our prefixes. When we observe different routes at the target AS T (through different neighbors) from multiple vantage points (*e.g.*, due to different routing preferences at different geographic locations), we run the algorithm for each vantage point separately. We can potentially execute this algorithm for each AS in the topology as the target AS. A similar experiment was performed by Colitti [8]; here, we use the same mechanism with a more diverse set of providers and with a different goal.

BGP poisoning does not work when BGP loop prevention is disabled. It may also not work when ASes filter poisoned announcements. These problems may prevent us from seeing all available neighbors and routes at the target AS. We discuss these limitations in Sec. 4.4.

Reverse engineering BGP decisions. We first announce an IP prefix from one PEERING location (called the *magnet*), wait five minutes to allow for route convergence, then announce (*anycast*) the same IP prefix from all other PEERING locations. After we anycast the prefix, An AS may change to a new route with higher LocalPref, shorter AS-path length, or better intradomain tie-breakers. If an AS keeps using the route toward the magnet after we anycast the prefix, the AS may be using route age as a tie-breaker (the last tie-breaker before router ID).

If the AS did not choose the route to the magnet, we check if the chosen route has a higher LocalPref or shorter AS length. If none of these checks are satisfied, we conclude that the BGP decision was made at an intermediate tie-breaker that considers the AS's intradomain topology. We repeat this process using each PEERING location as the magnet. We also check whether the route chosen after we anycast the prefix has a lower LocalPref or equal LocalPref but longer AS-path length; which is a violation of the Gao-Rexford model. The route to the magnet may become unavailable when a downstream AS receives and choses a more preferred route; in these cases we consider the downstream AS's decision.

Data set. We performed a total of 188 distinct prefix announcements to infer preferences for all 360 target ASes we observe on paths toward PEERING. We observe 739 inter-AS links, 45 (6.1%) of which are not in CAIDA's AS-relationship database.

3.3 Comparison with existing models

We compare paths observed in our our data- and control-plane measurements with CAIDA's topology of inferred inter-AS relationships. We aggregate 5 topologies (Oct 14 to Feb 15) inferred using the method presented by Luckie *et al.* [23]. We aggregate these snapshots of the AS level topology to mitigate the impact of transient link failures on the topology used in our analysis. When inferences conflicted, we took the majority poll of inferred relationships while assigning higher weight to more recent inferences. We use this topology to compute all paths that satisfy the Gao-Rexford (GR) local preference model described in Sec. 2.

We compare the measured paths with all paths satisfying the GR model of local preference computed using CAIDA's inferred relationships. We consider two properties: (1) whether the measured path satisfies the GR model of local preference, and (2) whether the measured path has the same length as the shortest paths satisfying the GR model of local preference. Based on this we classify routing relationships as either obeying GR local preference; *i.e.*, using the neigh-

[1] We targeted 2,000 probes but two did not return any data and had to be discarded.

bor with the Best Relationship type (**Best**), routing based on shortest path (**Short**), or a combination of the two.

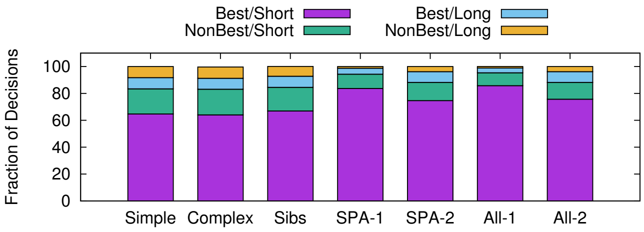
For control-plane measurements to discover alternate routes, we consider the order in which the target AS T chooses paths. Again, we consider two properties: (1) whether the relationship between T and the next-hop on the first path is equal or better than the relationship with the next-hop on the second path, and (2) whether the first path is shorter or equal in length as the second path. We similarly label the observed decisions which obey property (1) as **Best**, and those that obey (2) as **Short**.

In both cases, the sets should be treated as disjoint, with ASes that obey both Best and Short path policies appearing only in the **Best/Short** category. Observations which follow **neither** of these properties are considered inconsistent with existing models (*i.e.*, violations).

4. HOW OFTEN DO MODELS HOLD?

We now consider how empirically observed AS paths compare with those predicted by models using AS relationships inferred in [23]. We then investigate how often deviations can be explained by known sources of inaccuracies.

Encouragingly, we find that a majority of routing decisions (65%) are correctly inferred by the commonly used Best/Short model; however, a significant fraction (35%) are not. Figure 2 characterizes the observed routing decisions based on whether the path chosen is Best or Short. We find only a small number of cases (8%) where decisions can neither be explained by Best or Shortest path selection. In the following sections, we explore the reasons behind these decisions that differ from model-based predictions.



.

Figure 2: Breakdown of routing decisions observed taking into account the complex relationships.

4.1 Complex routing relationships

A well known limitation of existing routing policy models is the simplification of relationships into either customer-provider or settlement-free peering relationships. Recent work by Giotsas *et al.* aims to address this limitation by augmenting existing relationship inferences with cases of hybrid relationships (*i.e.*, ASes whose arrangements vary based on location) and partial transit relationships (*i.e.*, ASes who will behave as providers, but only for a subset of prefixes) [14]. Figure 2 (Complex) shows the breakdown of routing decisions observed taking into account these complex relationships. Interestingly, we find that taking these relationships has nearly no impact on the classification in our dataset.

4.2 Sibling ASes

The mapping between AS numbers and organizations is not one-to-one [5]. Many organizations manage multiple AS numbers, either for geographic regions (*e.g.*, Verizon with ASNs 701, 702, and 703) or due to mergers (*e.g.*, Level 3 (AS 3356) and Global Crossing (AS 3549)).

We take a similar approach to Cai et al. [5] to identify AS siblings, but our approach differs in two key ways. First, we focus only on e-mail addresses in whois data, which previous work identified as the field with best precision and recall [5]. Second, we use DNS SOA records to identify different e-mail domains that belong to the same organization. For example, dish.com and dishaccess.tv share the dishnetwork.com authoritative domain. We also remove groups where the e-mail address is hosted by a popular e-mail provider (*e.g.*, hotmail.com), or regional Internet registry (*e.g.*, ripe.net). This results in a total of 94 sibling groups identified in our traceroute data set.

For every non GR decision that an AS makes, we check whether the AS chose a path via a sibling. If the path is a via a sibling, we mark this decision as satisfying the Best condition. Figure 2 (Sibs) shows the result of this change—3% more decisions are classified as Best/Short.

4.3 Prefix-specific policies

Interdomain routing is often abstracted to the level of a destination AS. However, in practice routing is based done on IP prefixes which may be subject to different export policies by their originating AS (*e.g.*, forwarding prefixes hosting enterprise-class services to a more expensive provider). While Giotsas *et al.* consider partial transit [14], which is a type of prefix-specific policy, they do not explicitly consider per-prefix policies as implemented by origin ASes.

We use two criteria to identify origin-based prefix specific policies based on correlation with BGP data obtained from Routeviews/RIPE [2,30]. Given an origin AS (O), neighbor N and prefix P: **Criteria 1** do not assume the edge $N - O$ exists for prefix P unless we observe O announcing P to N in the BGP data. **Criteria 2** is similar to Criteria 1, except that we require that we observe at least one prefix announced from O to N before applying Criteria 1. The first criteria can be seen as being more aggressive whereas the second aims to ensure that our observation is actually caused by selective prefix announcement and not poor visibility.

Figure 2 (SPA-1, SPA-2) shows the breakdown of routing decisions using Criteria 1 and 2 above, respectively. We find that prefix-specific policies account for a significant fraction (10-19%) of unexpected routing decisions.

Validation. In order to validate cases of prefix-specific policies, we try to find a Looking Glass server hosted by the neighboring AS. There were a total of 630 cases of prefix-specific policies involving 149 unique neighboring ASes.

We were able to find looking glass servers in 28 of the neighboring ASes. Using these looking glass servers we manually verify 100 cases of prefix-specific policies and confirm that applying Criteria 1 was correct 78% of the time.

4.4 Active BGP Measurements

Our control-plane experiments allow us to check how often our models match real routing choices and how many routing decisions they capture.

Alternate routes. Here analyze AS routing choices when we use PEERING to discover alternate, less preferred routes. We compare the sequence of routes chosen by target ASes with CAIDA's AS-relationships database. Out of the 360 ASes we targeted, 310 (86.1%) chose routes following both Best and Shortest (as defined in Sec. 3.3); 29 (8.0%) chose routes following Best only; 18 (5.0%) following Shortest only; and 3 (0.8%) did not follow either properties. We now discuss the 3 observations that did not satisfy either property to illustrate limitations of current models.

One violation occurs for a European network E that chooses to route via OpenPeering (AS20562)–a partial-transit relationship validated using whois. After poisoning OpenPeering, E chooses a route through another settlement-free peer-to-peer relationship with AMPATH (AS20080) at AMS-IX. We list this as a violation because CAIDA identifies OpenPeering as a provider for E. Interestingly, the second route is the suffix of the first route (*i.e.*, the route through OpenPeering also reaches PEERING through AMPATH at AMS-IX), indicating the first route includes an unnecessary detour. Peering relationships are not only complex, one settlement-free (or paid) peering relationship may be preferred over another. Models with finer granularity for ranking neighbors of an AS may resolve these issues.

Another violation occurs at a US university U. The university first chooses a route through Internet2 (AS11537) toward one of the PEERING locations in the US. After we poison Internet2, U chooses a route through AMPATH (AS20080) toward the PEERING location in Brazil. We list this as a violation because CAIDA identifies Internet2 as a provider and AMPATH as a settlement-free peer of U. Our last observed violation is similar, where a European network first chooses a route through Switch (AS559, identified as a provider) and then chooses a route through NCSA (AS10764, identified as a settlement-free peer) to reach PEERING after we poison Switch. These violations indicate that identifying links used as back-up might improve our routing models.

Reverse engineering BGP decisions. We now turn to our second control-plane experiment, where we use anycast to explore considerations such as older path on routing decisions. Table 1 shows the root cause behind BGP routing decisions. Although most decisions are made based on relationship and path length, more than 15% of decisions are made based on intradomain factors and route age, which are not considered in current models.

CAUSE	BGP FEEDS		TRACEROUTES	
Higher LocalPref	435	(46.0%)	228	(42.4%)
Shorter path	152	(16.0%)	158	(29.4%)
Intradomain	155	(16.4%)	84	(15.6%)
Route age (magnet)	24	(2.5%)	9	(1.6%)
GR violations	179	(18.9%)	58	(10.8%)
Total	**945**	(100%)	**537**	(100%)

Table 1: Reverse engineering of the BGP decision process.

Limitations. We note our results for control-plane experiments cover a small fraction of the Internet and are probably biased toward academic and research networks. Our control-plane techniques, however, are general and could be used by other networks to cover different portions of the Internet. We believe better coverage and visibility would result in discovering more violations. To this end, we are working to extend the PEERING platform as well as talking with RIPE about using RIPE Atlas to monitor routes to PEERING prefixes.

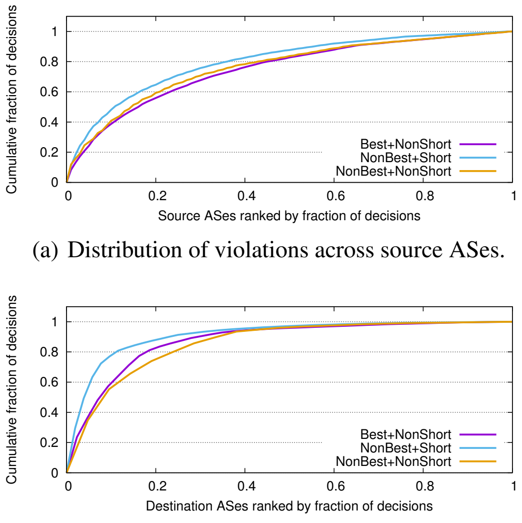
5. SOURCES OF VIOLATIONS

In this section we investigate which source and destination ASes account for most of the routing decisions which deviate from our model. Figure 3 (a) and (b) shows the cumulative fraction of routing decisions which violate either the Best or Short condition (*i.e.*, the AS chooses a path that is longer or more expensive than we would expect). If violations were evenly distributed across ASes, the curves would fix $y = x$; otherwise, some ASes are responsible for a disproportionately larger (or smaller) fraction of violations. We find this effect is present in both plots, but more prominently for destination ASes. We focus on the latter.

Destination ASes owned by Akamai account for 21% of violations. Of these, Cogent (AS174) is the most common source, responsible for 3.4% of violations. These Cogent-Akamai violations tend to occur when Cogent prefers a peer-to-peer path through a Tier-1 AS over a longer customer route. Netflix's AS is the destination on 17% or paths with violations. Of these, nearly a quarter (24%) are due to a stale inter-AS link in CAIDA's topology, which included a direct link between AS3549 and Netflix that no longer exists. For source ASes, the distribution is less skewed. Cogent and Time Warner are the top two sources, responsible for 4.1% and 2.2% of violations, respectively.

6. IMPACT OF GEOGRAPHY

We next consider the role of geography on routing decisions. First, we isolated traceroutes that stay within a continent (Continental traceroutes), *i.e.*, all hops stay inside a given continent based on geolocating router IP addresses. We use the geolocation data from [6], which offers good coverage of infrastructure IPs such as routers. Figure 4 shows the breakdown of decisions in the continental traceroutes (45% of those in our dataset). The fraction of decisions



(a) Distribution of violations across source ASes.

(b) Distributions of violations across destination ASes.

Figure 3: CDF plot of the fraction of violations (x-axis) explained by source and destinations ASes (y-axis). Violations observed in our dataset are skewed significantly toward Akamai and Netflix. The skew for source ASes is less prominent.

explained by GR for continental traceroutes is significantly greater than for transcontinental ones.

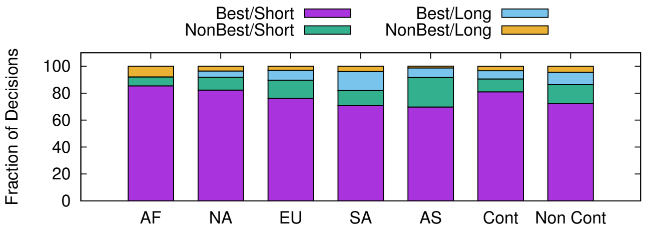


Figure 4: Breakdown of traceroutes that stay within a continent

Domestic paths. Next we focused on traceroutes where we infer that the entire traceroute stayed within a single country, but there is a better *multinational Best/Short path* (in the CAIDA data), which we define to be a path with at least one AS registered (via whois data) in a country outside the source and destination AS's country. We find that more than 40% of non-Best/Short decisions can be explained by avoiding alternative multinational paths. Table 2 details the non-Best/Short decisions explained by ASes preferring domestic routes.

Undersea cables. Undersea cable ASes are a critical component of Internet topologies that previous work overlooks. While some cables are jointly owned by large ISPs, e.g., Pan-American Crossing, Americas-II (owned by AT&T, Sprint, and many others), we observed that others, e.g., EAC- C2C (PACNET), are operated by independent organizations using their own allocated ASNs and IP prefixes. Because these cable operators only provide point-to-point transit along the cables (i.e., they do not originate traffic and peer in locations proportional to cable landings), they resemble high-latency, high-cost IXPs and thus confuse existing AS relationship models. As such, we need techniques to identify cable ASes and correct their relationships in inferred topologies.

We use a list of undersea cables from the TeleGeography Submarine Cable Map [1] to identify ASes for undersea cable operators. Overall, cable-ASes appear on less than 2% of paths but most of the decisions (51%) involving cable-ASes caused deviations from Best/Short paths. Table 3 shows fraction of each type of decision explained by undersea cable ASes.

Continent	Non-Best/Short Decisions explained
Asia	40.1%
Africa	62.5%
N. America	10.9%
Oceana	62.9%
S. America	66.6%

Table 2: Summary of Non-Best/Short decisions explained by ASes preferring intra-country routes.

Violation type	Pct. of decisions explained
Non-Best & Short	3%
Best & Long	6.5%
Non-Best & Long	4.5%

Table 3: Fraction of decisions of each type that can be attributed to undersea cables.

7. CONCLUSION

In this work, we investigated how interdomain paths predicted by state-of-the-art routing models differ from empirically observed routes. We found that while a majority of paths in our dataset agree with models, more than a third do not. We explained a significant fraction of these differences due to factors such as sibling ASes, selective prefix announcements and undersea cables. Further, we investigated how the models hold up when comparing with ground-truth routing preferences revealed using PEERING announcements, and identified AS behavior that is not included in existing models. As part of future work, we are continuing to investigate cases of routing decisions that violate today's models, and we aim to incorporate our findings into new models of Internet routing.

Acknowledgments

Research in this report was funded by NSF grant CNS-1423659 and a Comcast TechFund award.

8. REFERENCES

[1] TeleGeography Submarine Cable Map. `http://www.submarinecablemap.com/`.

[2] University of Oregon Route Views Project. `http://www.routeviews.org/`.

[3] H. Ballani, P. Francis, and X. Zhang. A study of prefix hijacking and interception in the Internet. In *SIGCOMM*, 2007.

[4] R. Bush, O. Maennel, M. Roughan, and S. Uhlig. Internet optometry: Assessing broken glasses in internet reachability. In *ACM IMC*, 2009.

[5] X. Cai, J. Heidemann, B. Krishnamurthy, and W. Willinger. Towards an AS-to-organization map. In *USENIX ATC*, 2010.

[6] B. Chandrasekaran, M. Bai, M. Schoenfield, A. Berger, N. Caruso, G. Economou, S. Gilliss, B. Maggs, K. Moses, D. Duff, K. NgâĂă, E. G. Sirer, R. WeberâĂă, and B. Wong. Alidade: Ip geolocation without active probing. *Department of Computer Science, Duke University, Technical Report*, 2015.

[7] K. Chen, D. Choffnes, R. Potharaju, Y. Chen, F. Bustamante, D. Pei, and Y. Zhao. Where the sidewalk ends: Extending the internet AS graph using traceroutes from P2P users. In *CoNEXT '09*, 2009.

[8] L. Colitti. *Internet Topology Discovery Using Active Probing*. Ph.D. thesis, University di Roma Tre, 2006.

[9] L. Gao, T. Griffin, and J. Rexford. Inherently safe backup routing with BGP. *IEEE INFOCOM*, 2001.

[10] L. Gao and J. Rexford. Stable Internet routing without global coordination. *Trans. Netw.*, 2001.

[11] P. Gill, S. Goldberg, and M. Schapira. A survey of interdomain routing policies. *ACM CCR*, 2014.

[12] P. Gill, M. Schapira, and S. Goldberg. Let the market drive deployment: A strategy for transistioning to BGP security. *SIGCOMM'11*, 2011.

[13] P. Gill, M. Schapira, and S. Goldberg. Modeling on quicksand: dealing with the scarcity of ground truth in interdomain routing data. *SIGCOMM Comput. Commun. Rev.*, 42(1):40–46, Jan. 2012.

[14] V. Giotsas, M. Luckie, B. Huffier, and K. Claffy. Inferring Complex AS Relationships. In *ACM IMC*, November 2014.

[15] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford. How secure are secure interdomain routing protocols? In *SIGCOMM'10*, 2010.

[16] T. Griffin, F. B. Shepherd, and G. Wilfong. The stable paths problem and interdomain routing. *Trans. Netw.*, 2002.

[17] G. Huston. Peering and settlements - Part I. *The Internet Protocol Journal (Cisco)*, 2(1), March 1999.

[18] G. Huston. Peering and settlements - Part II. *The Internet Protocol Journal (Cisco)*, 2(2), June 1999.

[19] U. Javed, I. Cunha, D. R. Choffnes, E. Katz-Bassett, T. Anderson, and A. Krishnamurthy. Poiroot: Investigating the root cause of interdomain path changes. In *SIGCOMM*, 2013.

[20] J. Karlin, S. Forrest, and J. Rexford. Nation-state routing: Censorship, wiretapping, and BGP. *CoRR*, 2009.

[21] C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian. Internet inter-domain traffic. In *SIGCOMM'10*, 2010.

[22] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang. PHAS: A prefix hijack alert system. In *Proc. USENIX Security Symposium*, 2006.

[23] M. Luckie, B. Huffaker, A. Dhamdhere, and V. Giotsas. AS relationships, customer cones, and validation. In *ACM Internet Measurement Conference*, 2013.

[24] R. Lychev, S. Goldberg, and M. Schapira. Is the juice worth the squeeze? BGP security in partial deployment. In *SIGCOMM'13*, 2013.

[25] H. Madhyastha, E. Katz-Bassett, T. Anderson, A. Krishnamurthy, and A. Venkataramani. iPlane Nano: Path prediction for peer-to-peer applications. In *Usenix NSDI*, 2009.

[26] R. Mazloum, M. Buob, J. Auge, B. Baynat, D. Rossi, and T. Friedman. Violation of Interdomain Routing Assumptions. In *Passive and Active Measurement Conference*, March 2014.

[27] W. Mühlbauer, A. Feldmann, O. Maennel, M. Roughan, and S. Uhlig. Building an AS-topology model that captures route diversity. In *SIGCOMM*, 2006.

[28] R. Oliveira, D. Pei, W. Willinger, B. Zhang, and L. Zhang. Quantifying the completeness of the observed internet AS-level structure. *UCLA Computer Science Department - Techical Report TR-080026-2008*, Sept 2008.

[29] Quantcast. `http://www.quantcast.com`.

[30] RIPE Network Coordination Center. RIPE Routing Information Service. http://www.ripe.net/data-tools/stats/ris/routing-information-service.

[31] M. Roughan, W. Willinger, O. Maennel, D. Perouli, and R. Bush. 10 lessons from 10 years of measuring and modeling the Internet's autonomous systems. *JSAC*, 2011.

[32] Sandvine. Fall 2012 global internet phenomena, 2012.

[33] B. Schlinker, K. Zarifis, I. Cunha, N. Feamster, and E. Katz-Bassett. PEERING: An AS for Us. In *Proc. ACM HotNets*, Los Angeles, CA, October 2014.

[34] J. Wu, Y. Zhang, Z. M. Mao, and K. Shin. Internet routing resilience to failures: Analysis and implications. In *CoNEXT*, 2007.