Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.055186

REVIEW

Internet Inter-Domain Path Inferring: Methods, Applications, and Future Directions

Xionglve Li, Chengyu Wang, Yifan Yang, Changsheng Hou, Bingnan Hou and Zhiping Cai*

College of Computer, National University of Defense Technology, Changsha, 410000, China

*Corresponding Author: Zhiping Cai. Email: zpcai@nudt.edu.cn

Received: 19 June 2024 Accepted: 26 August 2024 Published: 15 October 2024

ABSTRACT

The global Internet is a complex network of interconnected autonomous systems (ASes). Understanding Internet inter-domain path information is crucial for understanding, managing, and improving the Internet. The path information can also help protect user privacy and security. However, due to the complicated and heterogeneous structure of the Internet, path information is not publicly available. Obtaining path information is challenging due to the limited measurement probes and collectors. Therefore, inferring Internet inter-domain paths from the limited data is a supplementary approach to measure Internet inter-domain paths. The purpose of this survey is to provide an overview of techniques that have been conducted to infer Internet inter-domain paths from 2005 to 2023 and present the main lessons from these studies. To this end, we summarize the inter-domain path inference techniques based on the granularity of the paths, for each method, we describe the data sources, the key ideas, the advantages, and the limitations. To help readers understand the path inference techniques, we also summarize the background techniques for path inference, such as techniques to measure the Internet, infer AS relationships, resolve aliases, and map IP addresses to ASes. A case study of the existing techniques is also presented to show the real-world applications of inter-domain path inference. Additionally, we discuss the challenges and opportunities in inferring Internet inter-domain paths, the drawbacks of the state-of-the-art techniques, and the future directions.

KEYWORDS

Internet inter-domain paths; path inference; network measurement; network modeling

1 Introduction

The global Internet is a complex network that consist of ASes. The owners of the ASes are of different types, such as Internet service providers (ISPs), content providers, and companies that provide specialized services (e.g., the Starlink). Thus, different ASes may use heterogeneous equipments to build their infrastructures and have distinct configurations, which are determined by various considerations (e.g., cost, performance, and security).

The Internet inter-domain path information can be used for various purposes. As summarized in Fig. 1, it can help:

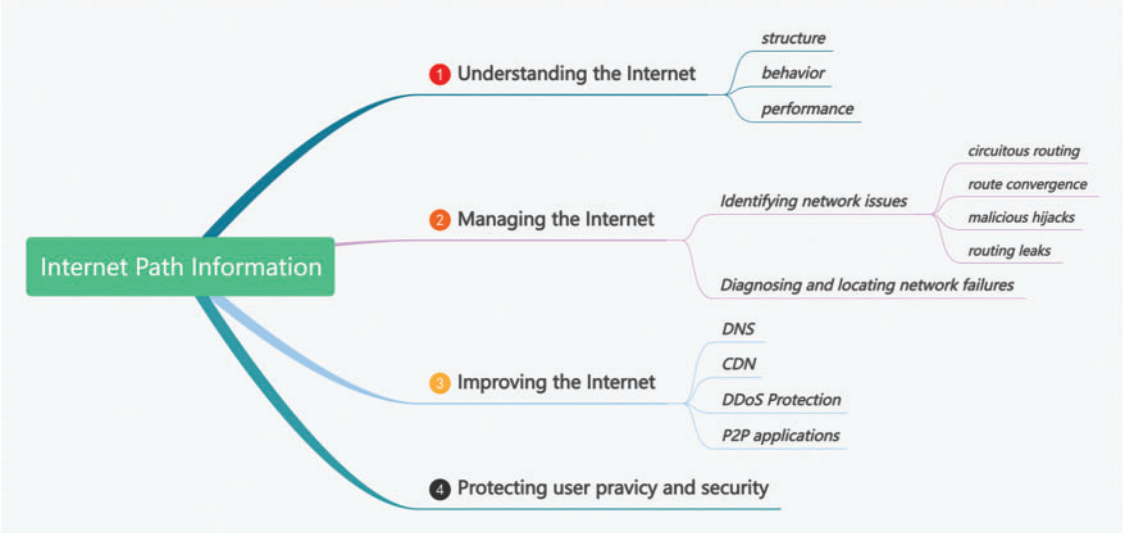

Figure 1: The use cases of Internet path information. The Internet path information can be used for various purposes, such as understanding the Internet structure [1–5], behavior [6–9], and performance [10–13]; managing the Internet for identifying network issues (circuitous routing [14], route convergence [15–17], malicious hijacks [18–20] and routing leaks [21]) and diagnosing [22–25] and locating [26,27] network failures; improving the Internet service and applications (DNS [28], CDN [29], DDoS protection [30], and P2P applications [31–34]); and protecting user privacy and security [35,36]

Understanding the Internet: the Internet inter-domain path information is crucial for network managers and operators to optimize the Internet's structure [1–5], which refers to the physical and logical arrangement of the network elements (such as routers, switches, links) and the connections between them; The path information can help us understand the network behavior [6–9], which refers to the activities and patterns exhibited by devices (such as routers, switches, servers) and applications during data transmission, processing, and communication. Analyzing network behavior helps identify normal and abnormal activities, ensuring network security and efficiency; The path information can also reveal the performance of the network [10–13], which refers to the quality of service provided by the network, such as latency, bandwidth, and packet loss.

Managing the Internet: the path information can be leveraged to identify network issues such as circuitous routing, where packets take unnecessarily long paths, increasing latency and packet loss [14]; route convergence issues, where unsynchronized routing tables cause loops and packet loss [15–17]; malicious hijacks, where attackers announce false routes to intercept traffic [18–20]; and routing leaks, where routes are improperly announced, diverting traffic along unintended paths [21]. Additionally, path information is valuable for diagnosing and pinpointing network failures, which occur when network elements malfunction, leading to unavailability or degraded performance [22–27].

Improving the Internet: the path information can help improve the performance of the Internet and foundation service Domain Name System (DNS) [28], it can also be used by Content Distribution Network (CDN) providers to optimize the content delivery [29], and it can be used by Distributed Denial of Service (DDoS) protection services to mitigate DDoS attacks [30]. Peer-to-Peer (P2P) applications can also benefit from path information [31–34].

Protecting user privacy and security: the path information can be used by end-users to protect their data privacy and security [35,36].

However, due to the complicated and heterogeneous structure of the Internet, different considerations of the organizations that own and operate the ASes, and the decentralized nature of the Internet, path information is not publicly available. Hence, to obtain path information, researchers and network operators have developed techniques to measure the Internet inter-domain paths. These techniques can be categorized into two types: active and passive. The most famous active measurement technique is the traceroute, which obtains the path from the probe to the destination by sending packets with increasing Time to live (TTL) values. Passive measurement techniques, such as router collectors to collect Border Gateway Protocol (BGP) tables, are also widely used to obtain path information. But the available measurement probes to perform active measurements or collectors to collect passive data are limited in number and coverage. Therefore, inferring Internet inter-domain paths from the limited data is a supplementary approach to measure Internet inter-domain paths.

In the field of network measurement, research on inferring Internet inter-domain paths has been extensive over the past two decades, there are several notable gaps in the literature. Firstly, there is no comprehensive survey that consolidates and summarizes the existing techniques for inferring these paths, making it difficult for researchers and practitioners to gain a holistic understanding of the field. Secondly, the applications of these techniques are not well documented or summarized, leaving a gap in understanding how these methods are being practically implemented and utilized. Finally, future directions for inferring Internet inter-domain paths have not been thoroughly discussed, limiting the ability to identify emerging trends and areas for further exploration. To fill these gaps, this survey reviews the existing techniques for inferring Internet inter-domain paths from 2005 to 2023 to provide a comprehensive overview of the state-of-the-art techniques, their applications, and future research directions in the field of Internet inter-domain path inference.

The contributions of this survey are as follows:

- This is the first survey that reviews the existing techniques for inferring Internet inter-domain paths. Not only does this survey summarize the existing techniques for inferring Internet inter-domain paths, but it also provides summaries of the fundamental techniques for Internet inter-domain path inference. With the introducing of fundamental techniques, the readers can understand the path inference techniques better.
- We have also conducted a case study to summarize the applications of existing techniques for inferring Internet inter-domain paths.
- By discussing the characteristics of the existing techniques, we aim to provide insights into the challenges and opportunities in modeling the Internet routing system to not only infer the paths but also predict the performance of the paths.

The rest of the paper is organized as follows. Table 1 summarizes the terms and concepts used in this survey. In Section 2, we show the taxonomy to exhibit the inter-domain path inference techniques. In Section 3, we introduce the fundamental techniques of inter-domain path inference to provide background information. In Section 4, we summarize the existing techniques for inferring Internet inter-domain paths. In Section 5, we present the case studies of the existing techniques to show real-world applications of inter-domain path inference. In Section 6, the challenges and opportunities in inferring Internet inter-domain paths, the drawbacks of the state-of-the-art technique, and the future directions are discussed. In Section 7, we conclude the paper.

Table 1: Summary of abbreviations, terms, and concepts

Abbreviations, terms, or concepts	Full names, definitions, or explanations
AS	Autonomous system
ISP	Internet service provider
DNS	Domain Name System
CDN	Content Distribution Network
P2P	Peer-to-Peer: applications allow users to share resources directly with each other without relying on a central server.
TTL	Time to live
BGP	Border Gateway Protocol
PoP	Point of Presence
NoC	Network-on-chip: an on-chip communication architecture that uses network principles to connect various components within a system-on-chip, enabling efficient data transfer and scalable communication between multiple processing cores and other functional units.
MPSoC	Multi-Processor System on Chip: An MPSoC integrates multiple processing cores and various functional units onto a single chip to handle complex tasks and applications efficiently.
NI	Network Interface: serves as a bridge between a chip or system and external networks, facilitating data transfer and communication.
On-chip router	An on-chip router manages data traffic between different components within a chip, enabling efficient communication and data exchange in multi-core and complex integrated circuits
RIPE NCC	Reseaux IP Europeans Network Coordination Center
CAIDA	Center for Applied Internet Data Analysis
RIS	Routing Information Service
RRC	Remote Route Collector
P2C or C2P	Provider-customer or customer-provider: a kind of AS business relationship
P2P	peer-peer: a kind of AS business relationship
S2S	sibling-sibling: a kind of AS business relationship
DDos	Distributed denial-of-service: a cyber-attack where the perpetrator seeks to make a network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
Valley free principle	A principle that summarized the routing policies of ASes, which states that the AS paths should not contain valleys, i.e., the traffic in an AS path can only be uphill or go downhill or go uphill and then downhill.
BGP atoms	A set of routers that route towards the Internet similarly.
Network tomography	A technique used to infer the internal structure and state of a network by observing its external behavior.
GPT	Generative Pre-trained Transformer: a type of deep learning model that uses unsupervised learning to pre-train a language model.

2 Taxonomy

Internet Paths at Different Levels: As described in [37], the Internet topology can be classified into four levels: AS-level, PoP-level (Point of Presence level), router-level, and IP-level. Accordingly, we classify the Internet inter-domain paths into four levels: IP-level, router-level, PoP-level, and AS-level. Fig. 2 is an overview of different levels of Internet inter-domain paths. We have reviewed the inter-domain path inference techniques based on the granularity of the paths they infer and found that most of the techniques infer AS-level paths, followed by PoP-level paths. Though some proposed techniques are capable of inferring IP-level and router-level paths, we did not find evaluation results these two levels of paths. The reasons could be: realizing high coverage for IP-level and router-level paths are more challenging due to the more fine-grained granularity means more measurement data is required.

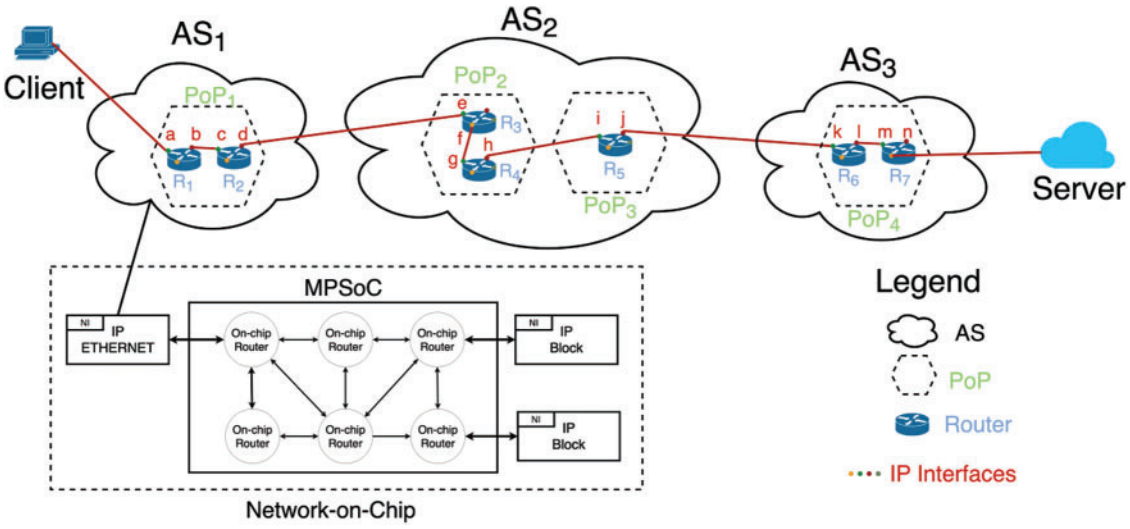

Figure 2: An overview of different levels of Internet paths. From the client C to the server S, the four levels of paths are: IP-level: *a-b-c-d-e-f-g-h-i-j-k-l-m-n*, router-level: R_1-R_2-R_3-R_4-R_5-R_6-R_7, PoP-level: PoP_1-PoP_2-PoP_3-PoP_4, AS-level: AS_1-AS_2-AS_3, where a, b, c, d, e, f, g, h, i, j, k, l, m, n are IP addresses, R_1, R_2, R_3, R_4, R_5, R_6, R_7 are routers, PoP_1, PoP_2, PoP_3, PoP_4 are Points of Presence (PoPs), and AS_1, AS_2, AS_3 are ASes. Besides the four levels of paths, with the emergence and widespread use of networks-on-chip, the paths at the network-on-chip level can also been seen as a new level of paths

Besides the four levels of paths, with the emergence and widespread use of networks-on-chip [38], the paths at the network-on-chip (NoC) level can also be seen as a new level of paths. The topic of networks-on-chip is very extensive and therefore requires a separate consideration, which is beyond the scope of this paper. It should only be noted that at the macro- and micro-level they are very similar to ordinary communication networks. For example, they can also be hierarchical, where signals at different levels of the hierarchy are transmitted in different transmission medium [39,40], and traffic routing methods are borrowed from classical networks [38,41]. On this basis, it can be argued, based on the principle of self-similarity in networks [42,43], that the conclusions that can be drawn for the AS_1, AS_2, AS_3... layers are also applicable for the NoC (see Fig. 2). A Multi-Processor System on Chip (MPSoC) is a unit that responsible for processing the network traffic within the chip and has similar network architecture with the ASes. The Network Interface (NI) can either be integrated into the MPSoC or function as an independent component. Regardless of its configuration, it serves as a

bridge between the external network and the on-chip network. The network traffic is processed by the NI and then enters the chip. In the chip, the entry traffic is transmitted by the on-chip routers based on the on-chip network.

From a Methodological Perspective: the inter-domain path inference techniques can be categorized into graph-based and stitching-based methods. The graph-based methods construct a graph with the data sources, such as BGP tables, and infer paths by searching the graph with some summarized regulars (e.g., valley-free principle). The stitching-based methods infer paths by stitching the path segments at the convergence points. Graph-based methods can achieve high coverage, but they are limited by the summarized regulars, which could not accurately capture the real routing behavior. For the stitching-based methods, the real routing behavior is captured by the path segments, but the coverage is limited by the availability of the path segments.

Data Sources: In network measurement, the measurement techniques are usually categorized into active methods and passive methods. Typical active methods include traceroute and ping, these methods measure the Internet by sending packets from the probes. Active measurement techniques generate extra traffic in the network, which may burden the network. Passive methods, such as BGP collectors, collect the data from the network without introducing extra traffic.

According to the path levels, inference method type, and data sources, we have summarized the path inference techniques in Table 2.

Table 2: Summary of Inter-domain path inference methods

Method type	Method name	Granularity	Data source
Stitching-based	iPlane [31]	PoP-Level and AS-Level	Traceroutes
Graph-based	iPlane Nano [32]	PoP-Level and AS-Level	BGP tables, traceroutes
Stitching-based	Sibyl [44]	PoP-Level and AS-Level	Traceroutes
Graph-based	RouteScope [45]	AS-Level	BGP tables and traceroutes
Graph-based	KnownPath [46]	AS-Level	BGP tables and traceroutes
Stitching-based	Path Stitching [34]	AS-Level	BGP tables and traceroutes
Graph-based	L-K AS Path Inference [47]	AS-Level	BGP tables
Stitching-based	HyperPath [33]	AS-Level	BGP tables
Graph-based	Policy-Preferred AS Path Enumeration [48]	AS-Level	BGP tables
Graph-based	PredictRoute [49]	AS-Level	BGP tables and traceroutes
Graph-based	RouteInfer [50]	AS-Level	BGP tables
Stitching-based	ProbInfer [51]	AS-Level	BGP tables
Graph-based	GMPI [52]	AS-Level	BGP tables

3 Fundamental Techniques for Internet Inter-Domain Path Inference

As shown in Table 3, the fundamental techniques of inter-domain path inference are composed of measurement techniques and auxiliary techniques. The measurement techniques provide the data sources for inferring Internet inter-domain paths, mainly including traceroute and BGP collectors. The auxiliary techniques are the techniques that assist the inter-domain path inference, mainly including techniques to infer AS business relationships, resolve aliases, and map IP addresses to ASes. It is worth noting that the auxiliary techniques may bring cumulative errors to inter-domain path inference. The reason is that the AS business relationships, aliased, IP-to-AS mapping are all inferred from the measurement data, which may contain errors. The errors in the auxiliary techniques will be propagated to the inter-domain path inference results. This survey does not focus on the above-mentioned techniques, but we summarize these techniques here to provide background information for the inter-domain path inference techniques.

Table 3: Fundamental techniques for Internet inter-domain path inference

Measurement techniques	Auxiliary techniques
Traceroute: Basic traceroute [53,54], reverse traceroute [55,56], fast traceroute [57], and multipath-aware traceroute [58]	AS business relationship inference: heuristic based methods [59–62] and data-driven based methods [63–66]
Measurement platform [67–70]	Alias resolution [71–75]
	IP-to-AS mapping [76–78]

3.1 Measurement Techniques

The measurement techniques for inferring Internet paths refers to techniques that provide the data sources for inferring Internet paths, mainly including traceroute and BGP collectors.

Traceroute: The traceroute is a widely used tool to measure the Internet inter-domain paths between the probes and the destinations. As shown in the Introduction, the obtained paths can be used for various purposes, such as understanding the Internet, managing the Internet, improving the Internet, and protecting user privacy and security. Besides the above-mentioned advantages, the traceroute can also contribute to IP geolocation [79,80].

Traceroute was first introduced by Van Jacobson in [53]. Over the decades, various modifications of traceroute have been developed to enhance the accuracy and efficiency of path measurement. However, the original traceroute may not be reliable when the network includes load-balancing routers, as packets might traverse different paths due to the load balancing. To address this issue, Paris traceroute [54] was introduced. In the paper proposing Paris traceroute, the authors highlight that load-balancing routers can lead to inaccurate path measurements by traceroute, categorizing the resulting anomalies into three types: "loops," "cycles," and "diamonds." To mitigate the effects of load-balancing routers, Paris traceroute varies the header fields of probe packets to ensure consistent path measurements, even in the presence of load balancing.

As illustrated in Fig. 3, the Internet is asymmetric. Paris traceroute can only measure the one-side path from the source to the destination. For most situations, the cooperation of the destination host is impossible, so the reverse path measurement is challenging. To overcome this challenge, Katz-Bassett et al. proposed a new technique called reverse traceroute [55]. The reverse traceroute aims to

provide accurate, scalable, and comprehensive path information from the target back to the source. Reverse traceroute can help network operators and researchers to troubleshoot performance issues, identify network topology, and measure link latencies effectively. The system architecture of reverse traceroute includes vantage points for measurements, a controller for coordination, and sources for path requests.

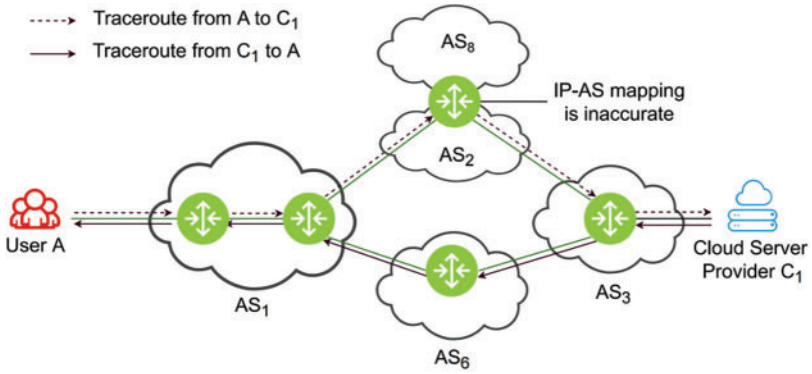

Figure 3: Due to the traffic engineering and asymmetric routing, the path from *S1* to *U1* is usually different from the path from *U1* to *S1*

Three techniques are leveraged in reverse traceroute to achieve the backward path: 1) Leveraging the destination-based nature of Internet routing to stitch the path hop-by-hop; 2) Utilizing the IP options to obtain the reverse path; 3) Employing a limited form of spoofing, which leads to the most strategically selected vantage point for the measurement.

The reverse traceroute technique faces limitations due to its high probe overhead, as discussed in Reference [56]. It can only map a small number of reverse paths each day, which is insufficient for conducting large-scale network analysis. To overcome this challenge, the REVTR 2.0 methodology is introduced in [56]. REVTR 2.0 offers enhanced throughput, accuracy, and coverage, rendering it suitable for performing reverse path measurements on an Internet-wide scale. The increased throughput is achieved by utilizing record route probes to map the initial nine hops (inclusive of the forward path), thereby efficiently identifying nearby vantage points. Moreover, by intersecting established routes in a traceroute atlas, the need for issuing additional probes can be minimized. Enhanced accuracy is ensured through a comprehensive measurement analysis demonstrating that presuming symmetry within an intra-domain hop is generally accurate, while assuming symmetry across inter-domain hops is not reliable. Leveraging this insight, REVTR 2.0 enhances precision by filtering out erroneous reverse traceroutes and marking potentially missing or unresponsive hops. The coverage is also expanded through the measurement analysis, which reveals that reverse paths often exhibit symmetry within an AS, providing more valuable data for reconstructing the reverse path.

The methods mentioned above are designed to achieve high coverage in path measurement. However, with the vast scale of the Internet, fast path measurement is also crucial. To address this, Yarrp [57] was introduced as a fast Internet router and link scanner. Yarrp's design employs a random probing strategy, where it randomly generates targets and sets the TTL of probe packets. Once the response packets are received, the topology information is analyzed offline. Yarrp is capable of achieving a high probing rate with low overhead, making it well-suited for large-scale network analysis.

Load-balanced forwarding paths pose a significant challenge for traceroute. To tackle this issue, a new technique called Diamond-Miner [58] has been introduced, offering a high-speed and

multipath-aware approach to traceroute. In addition to these advancements, Diamond-Miner also sheds light on the dynamics of the Internet, providing a taxonomy of load balancer remapping events with insights into their extent and prevalence.

With the above-mentioned techniques, traceroute is becoming faster, more accurate, and the path measurement scope is significantly broadened. However, the scale of measurement resources is still insufficient to measure paths between arbitrary pairs of hosts.

Border Gateway Protocol (BGP) is the de facto inter-domain routing protocol used in the Internet. The AS path attribute in BGP routing tables are advertised by BGP routers, which are used to make routing decisions. An AS path is a sequence of ASes that announce the route to the destination prefix. To help researchers and network operators to understand the Internet routing system, many owners of BGP routers collect BGP tables and make them publicly available. These public BGP tables are widely used by researchers to infer Internet inter-domain paths.

Measurement Platforms: The measurement platforms, such as RIPE NCC [67], CAIDA [68], Route Views [69], and PlanetLab [70], provide the measurement infrastructure for researchers to measure the Internet inter-domain paths.

Reseaux IP Europeans Network Coordination Center (RIPE NCC) is a regional Internet registry that provides both infrastructure to collect BGP tables and traceroutes and a platform to analyze the collected data. The RIPE Atlas [81] is a global network of over 12,000 active probes that can be used to measure Internet. The RIPE Routing Information Service (RIPE RIS) [82] is a distributed measurement infrastructure (Remote Route Collectors (RRCs)) that collects BGP tables from BGP routers. There are 23 active RRCs in the RIPE RIS network now and 3 historic RRCs.

Center for Applied Internet Data Analysis (CAIDA) is a research community that provides the measurement infrastructure to support large-scale data collection and data distribution to the scientific research community. The CAIDA Ark [83] is a project that measures the whole Internet with traceroutes. To measure the whole IPv4 address space, the CAIDA Ark project first divides the IPv4 address space by the/24 prefix, then randomly selects an IP address in each/24 prefix, and sends traceroutes to the selected IP addresses. The measurement is conducted by a team of 160 monitors and the data is made publicly available. The CAIDA AS Rank [84] is a project that ranks the ASes based on the number of IP addresses they announce. The data source of the AS Rank is the BGP tables collected by RIPE RIS and Route Views and the traceroutes collected by CAIDA Ark.

Route Views is a project supported by the University of Oregon, which aims to provide real-time BGP information about the global routing system to researchers and network operators. Route Views provides routing data since 1997, now it owns 47 BGP collectors.

PlanetLab is a global research network first appeared in 2002, which aims to support the creation of new network services. At the peak of its development, PlanetLab has 1353 nodes at 717 sites spread across 48 countries. The PlanetLab public the traceroute data collected during their measurement to the public.

Though there are many measurement platforms measures the Internet from different locations, the coverage of the measurement platforms is still limited. As mentioned in [85,86], we should note that the coverage limitation of the measurement infrastructure could lead to biased data collection, which may affect downstream analysis.

3.2 Auxiliary Techniques

AS Business Relationship Inference is a reverse-engineering process of the Internet routing system, which not only helps to understand the Internet but also provides insights into building a more optimized routing system. It's a worthy research topic in the field of network measurement and modeling. AS business relationships are widely used in inferring Internet inter-domain paths. Essentially, the AS business relationships are inferred relationships that represent the commercial relationships between ASes. The data sources for inferring AS business relationships include BGP tables and traceroutes.

In [59], AS business relationships are first categorized into three types: customer-provider (P2C or C2P), peer-peer (P2P), and sibling-sibling (S2S). The customer-provider relationship is a commercial relationship where the customer pays the provider for the transit service. The peer-peer relationship is a commercial relationship where the two ASes exchange traffic without payment. The sibling-sibling relationship is a commercial relationship where the two ASes are under the same organization.

Then, in [60], heuristic algorithms are proposed to infer AS relationships with BGP tables, which are based on the intuition that providers are typically larger than their customers, and peers are usually of comparable size. To infer the AS relationships, the authors proposed to represent AS relationships as a directed graph, where the nodes are ASes and the edges are the relationships between the ASes. Only edges between providers and customers are directed, while edges between peers and siblings are undirected. The authors also proposed the famous valley-free principle, which is widely used in inter-domain path inference to filter the possible paths. The valley-free principle is summarized as follows: 1) A provider-customer link can only be followed by provider-customer or sibling-sibling links. 2) A peer-peer link can only be followed by provider-customer or sibling-sibling links. With the above definition and the valley-free principle, different types of AS relationships are inferred with different algorithms.

In [61], in addition to BGP tables, traceroutes are introduced for inferring AS business relationships. The authors of [61] classified the AS relationships into four types: transit, peering, partial transit, and hybrid. The transit relationship is when an AS provides access to its providers, customers, and peers to another AS. In the peering relationship, two ASes share customer routes with each other. The partial transit relationship is when an AS provides another AS transit service to its customers and peers, but not to providers. The hybrid relationship is a combination of the above three relationships. The authors focus on the relationship inference of the partial transit and hybrid relationships, which are difficult to infer only with BGP tables. To address this issue, a new algorithm is proposed to infer these complex relationships, which utilizes BGP tables, traceroutes, and geolocation data. Their insight of identify the complex AS relationships and then tailor the inference algorithm to infer these relationships is a valuable contribution to the field of inferring AS relationships.

Problink [63] is a data-driven approach for inferring AS relationships. It begins by classifying the links between ASes into "easy" and "hard" categories based on the difficulty of inferring the relationships. To infer the hard relationships, a Naive Bayes classifier is employed. The benchmark for identifying these hard relationships is a heuristic algorithm called CoreToleaf, which infers AS relationships using the valley-free principle and Tier-1 ASes. Based on CoreToleaf's inference results, three factors have been identified as leading to the difficulty: 1) degree inversion, 2) violation of the valley-free principle, and 3) the instability of existing methods when applied to data from different vantage points and time periods. To address these challenges, Problink integrates various features of the links and the paths traversing them into a comprehensive probabilistic model.

Subsequent research [62,64] on inferring AS relationships has followed a similar approach to the earlier studies [61,63]: observing existing methods, identifying links that are difficult to infer, and then

developing new algorithms to address these hard-to-infer links. In [62], the hard links are those where the relationships cannot be conclusively determined by the principle-based algorithm they employed. The links that can be reliably inferred are primarily P2P links between Tier-1 ASes and P2C links downstream of Tier-1 ASes. In contrast, the hard links in [64] are those whose relationships cannot be identified using their voting algorithm. The challenges in inferring these hard links can be attributed to several factors: 1) biased data collection—since route collectors are not evenly distributed across the Internet, the data they collect may be skewed, revealing only a small portion of links between Tier-2 ASes and often missing many links between Tier-2 ASes and stub ASes, which contributes to the difficulty in inferring these links; 2) existing algorithms struggle with accurately identifying P2P links, often misclassifying them as P2C links; and 3) unreliable assumptions and heuristics, which increase the uncertainty of the inference results.

In recent years, the advancement of machine learning techniques has led to the development of machine learning-based methods for inferring AS relationships. For example, Reference [65] utilized graph neural networks to infer AS relationships, while BGP2VEC [66] embeds ASes into vectors and applies techniques from natural language processing for the same purpose. These data-driven approaches have demonstrated potential for improving the accuracy of AS relationship inference and offer a new perspective on the problem. However, they are constrained by the quality of the training data, the selection of features, and the choice of models. Additionally, the effectiveness of these methods is limited by the coverage of the training data, which depends on the measurement platforms used for data collection. As a result, the extent of the training data is inherently restricted by the capabilities and reach of these platforms.

Alias Resolution: As a router may have multiple IP addresses, The alias resolution techniques [71–75] are proposed to identify IP addresses that owned by the same router. The key idea of alias resolution is analyzing the IP IDs of the packets to find the IP addresses that allocated to the same router. The alias resolution techniques are widely used in inter-domain path inference to obtain the router-level paths from traceroutes. For example, in iPlane [31], iPlane Nano [32], and Sibyl [44], the alias resolution techniques are used to obtain PoP-level paths from traceroutes.

IP-to-AS Mapping techniques [76–78] are used to associate IP interfaces obtained from traceroutes with their corresponding ASes. A straightforward method for determining which AS an IP interface belongs to is the longest prefix match. To ensure that IP interfaces belonging to the same router are mapped to the same AS, alias resolution techniques are employed as part of the IP-to-AS mapping process.

4 Scoped Inter-Domain Path Inference Techniques

We first summarize the techniques that can both infer PoP and AS level paths, then the techniques that can only infer AS level paths. In each subsection, we first introduce the stitching-based methods, then the graph-based methods, the techniques are introduced in chronological order. We summarize each method from four aspects: the data sources, the key idea of how the method works, the advantages, and the limitations.

4.1 Inference Techniques for PoP and AS Level Paths

In theory, traceroute data based inter-domain path inference techniques can infer paths at different granularities, such as IP-level, router-level, PoP-level, and AS-level. However, the limited coverage of traceroutes makes it difficult to realize high coverage for IP-level and router-level paths. Therefore, the existing techniques mainly focus on inferring PoP and AS level paths.

Stitching-Based Methods: The iPlane [31] is an information plane aims to provide path and performance information between any two Internet hosts. The data sources of iPlane are traceroutes, which are collected by nearly a thousand of probes deployed in the Internet. iPlane is a stitching-based method that infers PoP and AS level paths by stitching the path segments at the convergence points. It works as follows: 1) iPlane first identifies the core routers and the links connecting them by active measurements, 2) then it identifies the edge routers and the links connecting them by opportunistic measurements, 3) finally, it stitches the path segments at the convergence points to infer the PoP and AS level paths. Besides the path inference, iPlane also provides the performance inference.

The iPlane is a pioneering work of the stitching-based path inference methods, which first introduces the stitching-based method to infer inter-domain paths. The advantages of iPlane are that it can infer paths at different granularities, such as PoP and AS level paths, and provide performance information. The limitation of iPlane is that the coverage is limited by the availability of the path segments, which may lead to inaccurate path inference results. The active measurements may also introduce extra traffic to the network, which may burden the network.

Sibyl [44] is a stitching-based method that developed based on iPlane. The key idea of Sibyl is to provide an Internet route oracle that allows users to issue rich queries expressed as regular expressions to obtain path information. It introduces a machine learning method to select the optimal path from the candidate paths, which improves the inference performance. The data sources of Sibyl are traceroutes, which are collected by real-time probes provided by RIPE Atlas. Sibyl introduces an algorithm to allocate the measurement budget to optimize the query satisfaction. Then it stitches the path segments as iPlane does to infer the PoP and AS level paths. At last, it uses a machine learning method to select the optimal path from the candidate paths.

The advantages of Sibyl are that it provides a more efficient way to allocate the measurement budget to optimize the query satisfaction and a machine learning method to select the optimal path from the candidate paths, which improves the inference accuracy. The limitation of Sibyl is that it also limited by the measurement probes.

Graph-Based Method: The iNano [32] is a system that can infer PoP and AS level paths with a compact Internet atlas, which is a representative graph-based inter-domain path inference method. The data sources of iNano are traceroutes measured by PlanetLab, which is the same as iPlane. After collecting the traceroutes, iNano maps the traceroutes to obtain different levels of paths to realize path inference at different granularities. An example of inferring path with iNano is shown in Fig. 4. iNano constructs an AS graph with the AS paths, and infers paths by searching the graph with the below regulars: 1) the collected 3-tuples from the AS paths, 2) the valley-free principle, and 3) summarized routing preferences stored as 3-tuples. The 3-tuple (AS_1, AS_2 > AS_3) means AS_1 prefers the path that goes through AS_2 over AS_3 to reach a destination, if the path is the same length. To obtain the PoP level paths, iNano stitches the PoP level path segments along the AS level paths.

The advantages of iNano are that it can achieve high coverage, as with most of the vertex pairs in the constructed graph are connected. The storage of the Internet atlas is less than 7 MB in the year of 2009, making it possible to be distributed to end-hosts. Besides the advantages, the limitations of iNano are that it is limited by its Internet routing model, which cannot handle the complex routing policies. The IP-to-AS mapping and alias resolution both introduce errors to the path inference on different levels.

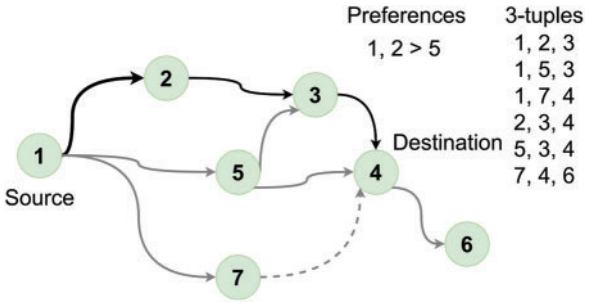

Figure 4: Inferring path from S to D with iNano, which is a representative graph-based method. The inferred path is AS_1-AS_2-AS_3-AS_4. It does not select the path AS_1-AS_5-AS_3-AS_4 as AS_1 prefers the path that goes through AS_2 over AS_5 to reach AS_4. The path AS_1-AS_5-AS_4 cannot be selected as the 3-tuple does not appear. The path AS_1-AS_7-AS_4 cannot be selected as the valley-free principle is violated

4.2 Inference Techniques for AS Level Paths

Stitching-Based Methods: In [34], Lee et al. proposed a novel approach called path stitching, which is designed to estimate end-to-end delay between hosts, the AS level path between the source and destination is also inferred in the process to estimate the delay. The data sources of this study are BGP tables from Route Views and RIPE RIS and traceroutes from CAIDA Ark. Its path and delay estimation is achieved by three steps: 1) inferring the AS level path between the source and destination, 2) stitching the traceroute segments along the inferred AS path, 3) estimating the delay by stitching the delay of traceroute segments along the inferred AS path.

The advantage of path stitching is that it introduces a new way to identify the first AS hop with the help of traceroutes, which significantly improves the AS level inter-domain path inference accuracy, which has been proved in the evaluation. Path stitching is also limited by the measurement probes, as the coverage of the measurement probes is limited, the path stitching may not be able to infer the path between arbitrary pairs of hosts.

In [33], Tao et al. explored AS inter-domain path inference in networks and introduces new algorithms, HyperPath and Valley-free HyperPath, leveraging the hyperbolicity property of the Internet. The concept of hyperbolicity is defined as a measure of how tree-like a graph is, which is derived from the field of geometric group theory and negatively curved metric spaces. Lower hyperbolicity of a graph indicates more tree-like properties. The data sources of HyperPath are BGP tables from Route Views. As shown in Fig. 5, HyperPath infers AS paths by stitching the path segments at the convergence points. More specifically, to infer the AS path between two prefixes p_1 and p_2, HyperPath first obtains k pairs of AS paths originating from k vantage ASes, each pair of paths starting from a same vantage AS and ending at two prefixes. Then, it selects the path with the minimum hop count among the k pairs of AS paths as the inferred AS path between the two prefixes. The valley-free HyperPath is an extension of HyperPath, which filters the possible paths with the valley-free principle in the path selection process. The evaluation shows that the valley-free HyperPath achieves higher accuracy than HyperPath.

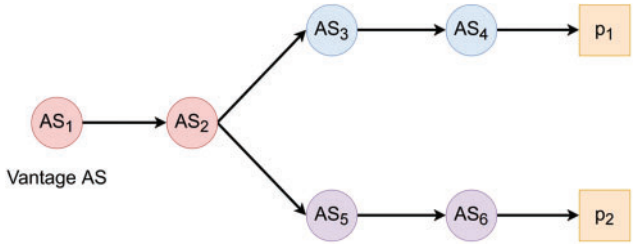

Figure 5: Toy example of HyperPath, a representative stitching-based path inference method. Two paths originating from the same vantage AS (AS_1) and ending at two prefixes (p_1 and p_2) are shown. The inferred AS path between p_1 and p_2 is $p_1 \rightarrow AS_4 \rightarrow AS_3 \rightarrow AS_2 \rightarrow AS_5 \rightarrow AS_6 \rightarrow p_2$, which is obtained by stitching the path segments of the two paths at the convergence point AS_2

The advantage of this study is that it provides a new perspective to infer AS paths by leveraging the hyperbolicity property of the Internet. It provides theory support for the stitching-based path inference methods. The main limitations of HyperPath and Valley-free HyperPath are that 1) they are not scalable, as for some prefix pairs, it is difficult to find path segments that converge at the same AS, and 2) they do not consider asymmetric of the Internet, which may lead to inaccurate inter-domain path inference results.

Graph-Based Methods: RouteScope [45] is a graph-based method that can infer AS-level between two ASes. The data sources of RouteScope are BGP tables and traceroutes from multiple vantage points. The key idea of RouteScope is to construct an AS graph with the AS paths obtained from BGP tables, then calculate the shortest paths between the source and destination ASes. The valley-free principle is used to filter the possible paths. The evaluation shows that the AS relationships filtering significantly improves the accuracy of AS inter-domain path inference.

RouteScope is a representative graph-based method that introduces the valley-free principle to filter the possible paths, it also firstly proposes to identify the first AS hop with the help of traceroutes. The limitation of RouteScope is that its shortest path and valley-free principle-based path inference may not be able to handle the complex routing policies of current Internet. The way to identify the first AS hop with traceroutes is limited by the number and distribution of measurement probes and the staleness of the traceroutes

KnownPath [46] is a graph-based method that infers AS-level paths by expanding AS paths that collected from BGP tables. The data sources of KnownPath are BGP tables from organizations such as Route Views and RIPE RIS. KnownPath first constructs an AS graph with the collected AS paths. Then, it uses a Bellman-Ford algorithm to expand the AS paths that directed to the same destination prefix. At the expanding step, the possible paths are filtered with the valley-free principle and sorted by weight. The weight of a path is the length of the sure part, which exists in real BGP tables.

KnownPath can be seen as a combination of the stitching-based and graph-based methods, where the known AS path segments are stitched to inferred path segments from a graph. The combination inherits the routing information from existing AS paths and the flexibility of the graph-based methods. The limitation of KnownPath is that it is limited by the availability of the known AS paths, which may lead to significant performance degradation when the known AS paths starting from an AS are limited.

The research [47] proposed a weighted graph-based method to infer AS paths. The data sources of this study are BGP tables from Route Views and CAIDA. The key idea of this study is to construct a weighted AS graph with the AS paths obtained from BGP tables, where the weight of the edges in the

AS graph is the frequency of the links in the BGP tables. The shortest paths between the source and destination ASes are calculated, then the valley-free principle is used to filter the possible paths. The evaluation shows that the AS relationships filtering significantly improves the accuracy of AS inter-domain path inference, especially for longer AS paths. The edge weight just reflects the frequency of the links in collected BGP tables, which may be biased by the route collectors.

The study [48] was a novel algorithm for policy-preferred path enumeration in a constructed AS graph. The data sources of this study are BGP tables from Route Views and RIPE RIS. In this study, four types of policies are used to summarize routing behavior from BGP tables: 1) explicit business relations, 2) valley-free principle, 3) the preferred first hop, and 4) the shortest path. The algorithm enumerates the policy-preferred inter-domain path inference to obtain a rooted, directed, acyclic graph for each destination AS. The policy-based Internet routing model is still suffering from the complexity of the Internet and biased data collection, which may lead to inaccurate path inference results.

In [49], PredictRoute is introduced, it constructs a probabilistic model for each destination prefix or AS to infer AS paths towards the destination. The data sources of PredictRoute are traceroutes from CAIDA Ark or any other traceroute measurement platform. The system constructs per-destination probabilistic Markov models based on traceroutes and uses supervised learning to improve inference accuracy by choosing between multiple possible paths. PredictRoute infers paths from ASes to a destination prefix by the trained Markov model for the destination prefix. If the Markov model for the destination prefix cannot provide a path, PredictRoute falls back to the BGPSim model [87] to guarantee a inter-domain path inference result. Inferring inter-domain AS-level paths with traceroutes inborn the limitation of inaccurate IP-to-AS mapping. The limited traceroutes is also a challenge for the traceroute-based path inference methods.

ProbInfer [51] is derived from HyperPath [33], but improves the candidate path selection process with a probability-based method. The data sources of ProbInfer are BGP tables from Route Views. ProbInfer builds a multigraph with the AS paths obtained from BGP tables, each path segment is considered as an edge in the multigraph. Thus, the path stitching process is transformed into finding common neighbors for the input ASes in the multigraph. After obtaining the candidate paths, ProbInfer uses a decision tree model to choose the optimal path from the candidate paths. The decision tree model is trained with features extracted from the candidate paths, such as the length of the path, the degrees of the ASes in the multigraph and global Internet, and the geolocation of the ASes.

The advantage of ProbInfer is that it proposes to separate the input AS pairs into SingleShortest and MultiShortest types, where SingleShortest means, for the input AS pair, there is only one shortest path in the candidate paths, and MultiShortest means there are multiple shortest paths in the candidate paths. Two separate decision tree models are trained to finish the path selection process for different types of AS pairs. The limitation of ProbInfer is that it is limited by the availability of the known AS paths, which may lead to significant performance degradation when the known AS paths starting from an AS are limited.

RouteInfer [50] is a heuristic-based algorithm that infers AS paths with AS graph constructed by data from the BGP tables. The data sources of RouteInfer are BGP tables from Route Views, RIPE RIS, and Isolario [88]. RouteInfer involves a data-driven method to serve as a fallback when the heuristic-based algorithm cannot make a decision. RouteInfer uses a 3-layer policy model to summarize routing behavior from BGP tables, the valley-free principle is also used to filter the possible paths. The 3-layer policy model is obtained by 3 steps: 1) Extracting prefix policies, which stores the preferences that ASes have for the paths to reach the prefixes; 2) Policy aggregation to obtain destination AS policies, which is used when the prefix policies is missing; 3) Policy aggregation to obtain neighbor AS policies, which

is used when the destination AS policies is missing. When the 3-layer policy model cannot capture any policy for an AS, RouteInfer falls back to a route decision model to predict the route decisions of the AS.

The advantage of RouteInfer is that it provides a fallback mechanism when the heuristic-based algorithm cannot make a decision, which significantly improves coverage. The limitation of RouteInfer is that it does not provide a portion of ASes that fall back to the data-driven method.

In [52], Li et al. introduced a generative and measurable path inference (GMPI) process, which is a data-driven process based on BGP tables.The data sources of GMPI are BGP tables from Route Views and RIPE RIS. The key contribution of GMPI is it creatively proposes a method to process the AS paths with intelligent ways, which unearthed the routing information concealed in the AS paths. The architecture and working process of GMPI are shown in Fig. 6, which is composed of four parts: Raw AS knowledge base, path generator, path feature extraction model, and path verisimilitude estimator. The working process of GMPI is as follows: 1) collecting raw AS knowledge and pre-processing the data, 2) generating k paths for each input AS pair with a heuristic path generation method, 3) encoding the AS paths to vectors, 4) estimating the likelihood of the generated paths. The heuristic path generation process generates paths for an input AS pair with the help of AS relationships, AS path frequency, and AS Rank [84]. The path representation and likelihood estimation are realized with dual-attention networks, which 1) first represents the ASes with graph embedding and AS rank features, 2) then encodes the sequential AS paths with a self-attention mechanism based network to capture vector representations of the AS paths, and 3) finally estimates the likelihood of the generated paths with another attention mechanism based network.

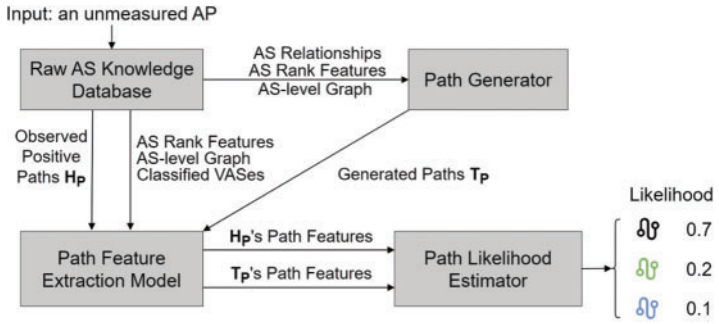

Figure 6: Architecture and working process of GMPI

GMPI first proposes to process the AS paths with intelligent ways, which unearthed the routing information concealed in the AS paths. It also provides a bridge to input the AS paths to the neural network models. The limitation of GMPI is that it may face the cold start problem when the observed data of an AS is limited, i.e., lacking of data to train an effective model for the AS. The high training cost is also a challenge for GMPI, as it trains a separated model for each AS to infer path from this AS to other ASes.

5 Case Study

This section introduces several case studies to demonstrate the application of inter-domain path inference techniques in various scenarios.

Detouring around failures: Detouring routing [89] is a technique used to reroute traffic when the direct path is unavailable. As summarized in [32], detouring routing can be implemented in three ways:

1) constantly monitoring paths between each pair of hosts, 2) constantly monitoring paths between each pair of detour nodes and routing hosts through nearby detour nodes, and 3) randomly selecting a small set of detour nodes. However, these methods are not efficient enough to be scaled effectively across the entire Internet.

The inter-domain path inference can be used to improve the efficiency of the detouring routing. When the direct path is unavailable, authors of iNano use the inter-domain path inference to obtain the path from the source to the target, the detour path via each available intermediary is also inferred by iNano. The detour paths are then ranked by the number of common PoPs and ASes between detour path and the inferred path. The detour path with the least common PoPs and ASes is chosen as the detour path. The evaluation shows that the detouring routing with the help of inter-domain path inference can reduce the fraction of cases when the destination is unreachable by roughly a factor of 2.

Inter-domain traffic reduction for BitTorrent P2P system: In [33], the authors proposed a method to reduce the inter-domain traffic for the BitTorrent P2P system with the help of inter-domain path inference. The authors first infer the AS paths between the peers with the proposed HyperPath and Valley-free HyperPath methods. Then the authors simulate the BitTorrent system with the inferred AS paths. The simulation results show that the Valley-free HyperPath method only introduces 21% additional traffic, while the random selection strategy introduces 89% extra traffic.

Inferring BGP atoms: The inter-domain path inference can be used to infer BGP atoms, which are a set of routers that route towards the Internet similarly. The PredictRoute [49] is a system that can infer AS paths towards a destination prefix or AS with the Markov chains. It provides a view of the routing behavior of all prefixes on the Internet, by comparing the graph similarity of the prefixes, the BGP atoms can be inferred.

Traffic engineering: The inter-domain path inference can be used to optimize the traffic engineering of the network. Network operators can utilize the inferred inter-domain path information to predict the impact of doing path prepending.

Protecting the privacy of the Internet users: The inter-domain path inference can be used to protect the privacy of the Internet users. As illustrated in Fig. 7, with the inferred inter-domain path information, user A can select the cloud server that does not traverse the ASes that user A does not trust.

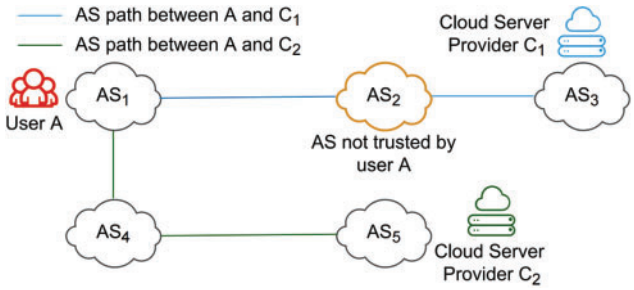

Figure 7: Illustration of how the inter-domain path inference can be used to protect the privacy of the Internet users

6 Discussion

6.1 Challenges and Opportunities

Though the inter-domain path inference techniques have been widely studied, there are still challenges and opportunities in inferring Internet inter-domain paths.

Granularity of Paths: The existing inter-domain path inference techniques mainly focus on inferring AS-level paths, followed by PoP-level paths. The inference of IP-level and router-level paths is still challenging due to: 1) lacking sufficient traceroutes to realize high coverage for IP-level and router-level inter-domain path inference; 2) Internet inter-domain paths change frequently at the IP-level, which makes it difficult to infer IP-level paths accurately. To realize high coverage and accuracy in inferring IP-level and router-level paths, further research is needed to develop techniques that can cope with the above challenges. To overcome the above challenge, we think the following aspects should be considered: 1) more BGP collectors and traceroute probes should be deployed to as many ASes as possible to collect more measurement data, 2) techniques to face the situation that many routers do not respond to the traceroute should be developed, 3) techniques to identify stale traceroute should be taken into account in IP-level inter-domain path inference, and 4) techniques to identify the alias IP addresses should be developed to obtain more accurate router-level paths.

Excessive Reliance on AS Business Relationships: The existing inter-domain path inference techniques heavily rely on the AS business relationships to filter the possible paths. However, 1) in actual Internet routing, AS paths that violate the valley-free principle do largely exist [90]. 2) Currently, the inferred AS relationships are mainly validated with relationships extracted from BGP communities [91], which is a best-effort ground-truth. Hence, the inferred AS relationships may be biased, and the biased results will be additive to the downstream tasks (e.g., the inter-domain path inference task). Thus, to reduce excessive dependence on AS business relationships, we can consider the following aspects: 1) develop techniques that can model the Internet routing system more accurately than the valley-free principle, 2) develop techniques that can obtain more accurate AS relationships, and 3) develop techniques that can cope with the AS paths that violate the valley-free principle.

Biased Data Sources: The existing inter-domain path inference techniques mainly use BGP tables and traceroutes as data sources. Currently, the BGP tables are collected by a few organizations, such as the Route Views project and RIPE RIS project, and the probes to perform traceroutes only deploy in a small part of ASes. So, the obtained measurement data is only a small part of the Internet from the view of the probes. The biased data sources may lead to biased path inference results, for example, if we cannot observe any path starting from an AS s, the path inference performance of the paths starting from s will be very poor. The performance degradation will also be observed on stitching-based methods, as the path segments starting from s are limited. Thus, to realize high coverage and accuracy in inter-domain path inference, new data sources or methods to cope with the biased data sources are needed. Below are the aspects that should be considered to reduce the bias of the data sources:

From the perspective of data collection, more vantage points should be deployed to collect more measurement data, this should be a joint effort of the Internet community, the more organizations and researchers public their measurement data, the more comprehensive the measurement data will be.

From the perspective of fully exploiting the existing data, 1) the historical BGP data should be fully exploited to serve the inter-domain path inference today. The research [92] that focus on inter-domain stability of BGP dynamics showed that the routing policies of ASes are relatively stable, more than 95% of the AS paths are stable for at least one week, and over 85% of the AS paths are stable for at least

one month. Thus, developing techniques that can extract useful information from the historical data to infer the current paths is a promising direction. 2) Accordingly, to the traceroutes, the stale traceroutes should be identified and filtered to obtain more accurate paths. 3) For the machine learning-based methods, the data augmentation techniques and the transfer learning techniques can be considered to cope with the biased data sources.

Privacy and Security: The inter-domain path inference techniques may bring privacy and security issues. For example, the inter-domain path inference techniques may infer the paths of the sensitive services, such as the financial services, which may bring security risks. To protect the privacy and security of the Internet users, the inter-domain path inference techniques should be designed with privacy and security in mind.

6.2 Drawbacks of the State-of-the-Art Technique

Though the state-of-the-art inter-domain path inference technique GMPI has made significant progress in inferring Internet inter-domain paths, there are still some drawbacks:

Cold Start Problem: The training formulation of GMPI is a typically supervised learning problem, which needs numerous labeled data (collected AS paths that starting from the source AS). The cold start problem may occur when the labeled data is insufficient, i.e., the inference accuracy is low for the Vantage ASes that can only collect a few paths starting from them.

High Training Cost: The GMPI trains a separated model for each AS to infer path from this AS to other ASes. Considering the huge number of ASes in the Internet, training a model for each AS is a high cost.

6.3 Future Directions

Though path information has shown its importance in network management, application performance optimization, and security, operators and researchers are not only interested in inferring paths but also in obtaining the performance information of the paths. Currently, a few inter-domain path inference techniques, such as iPlane, iNano, and Sibyl, have realized the path and performance inference. However, the existing techniques obtain the performance information by adding the performance along the path segments, which may not reflect the actual performance of the paths. More importantly, the performance information is not available for all the paths. Therefore, a future direction is to develop techniques that can realize the path and performance inference for more paths and more accurately.

To realize the path and performance inference more accurately and efficiently, the following technique routes should be considered:

The first possible future direction is to combine the inter-domain path inference techniques with the network tomography techniques to realize the path and performance inference more accurately and efficiently. Network tomography is a technique used to infer the internal structure and state of a network by observing its external behavior. It's analogous to medical tomography, like X-ray computed tomography (CT scans), where internal body structures are reconstructed from multiple external measurements. Network tomography techniques [93–96] have been widely studied to infer the performance of the networks for decades. Recently, neural tomography [97] has emerged as a promising method for inferring the performance of networks with unknown internal structures (i.e., without requiring direct knowledge of the underlying network topology). This technique utilizes neural networks to model and predict end-to-end performance metrics such as latency, throughput, and packet loss. By learning from

observed data, neural tomography effectively captures complex patterns and interactions within the network, making it particularly useful in scenarios where traditional methods fall short. The approach has demonstrated impressive accuracy and reliability in predicting network performance, highlighting its potential as a powerful tool for network analysis and optimization.

The second possible future direction is combining the inter-domain path inference techniques with the network modeling and performance prediction techniques to realize the model of the Internet routing system. Network modeling and performance prediction techniques [98–102] have been widely studied to model the network traffic and predict the network performance. These data-driven techniques embed the network topology, traffic propagation paths, and flow characteristics into the models and predict the network performance. But the existing techniques in this area can only work on small networks, such as data center networks. Hence, the key to combining the inter-domain path inference techniques with the network modeling and performance prediction techniques is to develop network modeling and performance prediction techniques that can work on large-scale networks, such as the network of an AS. Then, the inter-domain path inference techniques can be combined with the network modeling and performance prediction techniques to realize the model of the Internet routing system, not only inferring the paths but also predicting the performance of the paths.

The third possible future direction is to leverage the large models. The large models, such as the GPTs [103,104], has shown amazing performance in natural language processing, which can generate human-like text. The large models can also be used to model the Internet routing system, as GMPI has proposed the way to encode the AS paths to vectors to feed the neural network models, a possible way is to leverage the large models to model the Internet routing system, both the inter-domain paths and the performance of the paths.

7 Conclusion

In this survey, we have provided a comprehensive overview of the existing techniques for inferring Internet inter-domain paths, which is a common research topic in the field of network measurement. In this survey, we first introduce the taxonomy of the Internet inter-domain path inference techniques, which are divided into AS-level, PoP-level, router-level, and IP-level path inference techniques. From the perspective of how the methods work, the techniques are divided into stitching-based and graph-based methods.

Then, the fundamental techniques for inferring Internet inter-domain paths are summarized, including the techniques to measure the Internet, infer AS relationships, resolve aliases, and map IP addresses to ASes. By introducing the fundamental techniques, we have provided background knowledge for understanding the existing techniques for inferring Internet inter-domain paths. After that, we summarize the existing techniques for inferring Internet inter-domain paths from four aspects: the data sources, the key idea of how the method works, the advantages, and the limitations. Followed by the summary, we have provided a case study to show the application of the inter-domain path inference techniques in different scenarios. Finally, we have discussed the challenges and opportunities in inferring Internet inter-domain paths, the drawbacks of the state-of-the-art technique, and the future directions in modeling the Internet routing system, which is to combine the inter-domain path inference techniques with the network modeling and performance prediction techniques to realize the model of the Internet routing system.

Acknowledgement: The authors would like to express their gratitude to the editors and reviewers for their detailed review and insightful advice.

Funding Statement: This work is supported by the China Postdoctoral Science Foundation (2023TQ0089), the National Natural Science Foundation of China (Nos. 62072465, 62172155), the Science and Technology Innovation Program of Hunan Province (Nos. 2022RC3061, 2023RC3027).

Author Contributions: Study conception and design: Xionglve Li and Chengyu Wang; draft manuscript preparation: Xionglve Li, Chengyu Wang, Yifan Yang and Changsheng Hou; supervision: Bingnan Hou and Zhiping Cai. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: This article does not involve data availability, and this section is not applicable.

Ethics Approval: This study did not involve any ethical issues, as it did not include human or animal subjects.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] G. Fei, Z. Li, Y. Zhou, X. Zhai, J. Ye and G. Hu, "Efficiently measure the topologies of large-Scale networks under the guidance of neural network gradients," *IEEE Netw. Lett.*, vol. 5, no. 4, pp. 250–254, Dec. 2023. doi: 10.1109/LNET.2023.3301008.

[2] P. Seehofer, R. Bless, H. Mahrt, and M. Zitterbart, "Scalable and efficient link layer topology discovery for autonomic networks," in *Proc. Int. Conf. Netw. Serv. Manag.*, Niagara Falls, ON, Canada, Oct. 2023, pp. 1–9.

[3] M. Gouel, K. Vermeulen, M. Mouchet, J. P. Rohrer, O. Fourmaux and T. Friedman, "Zeph & Iris map the internet: A resilient reinforcement learning approach to distributed IP route tracing," *Comput. Commun. Rev.*, vol. 52, no. 1, pp. 2– 9, Jun. 2022. doi: 10.1145/3523230.3523232.

[4] R. Motamedi, B. Yeganeh, B. Chandrasekaran, R. Rejaie, B. M. Maggs and W. Willinger, "On mapping the interconnections in today's Internet," *Trans. Netw.*, vol. 27, no. 5, pp. 2056–2070, Oct. 2019. doi: 10.1109/TNET.2019.2940369.

[5] X. lve Li, J. Xi, Z. Cai, T. Yang, and C. F. Cheang, "Analyzing the structure and connectivity of continent-level Internet topology," *Comput. Mater. Contin.*, vol. 59, no. 3, pp. 955–964, Jan. 2019. doi: 10.32604/cmc.2019.05769.

[6] Y. Kuang, D. Li, X. Huang, M. Zhou, and W. Wang, "PoiEvent: An approach to extract the persistent and destructive routing events," *Comput. Netw.*, vol. 217, Oct. 2022, Art. no. 109313. doi: 10.1016/J.COMNET.2022.109313.

[7] A. Marder, K. Claffy, and A. C. Snoeren, "Inferring cloud interconnections: Validation, geolocation, and routing behavior," in *Proc. Int. Conf. Passive Active Meas*, Cottbus, Germany, Mar. 2021, pp. 230–246.

[8] M. D. Bartolomeo, V. D. Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, "Extracting routing events from traceroutes: A matter of empathy," *Trans. Netw.*, vol. 27, no. 3, pp. 1000–1012, Jul. 2019. doi: 10.1109/TNET.2019.2911330.

[9] R. A. Steenbergen, "A practical guide to (correctly) troubleshooting with traceroute," presented at the 47th North Am. Netw. Oper. Group, Dearborn, MI, USA, Oct. 18–21, 2009.

[10] O. V. Babasanmi and J. Chavula, "Measuring cloud latency in Africa," in *Proc. Int. Conf. Cloud Netw.*, Paris, France, Nov. 07–10, 2022, pp. 61–66.

[11] L. Corneo *et al.*, "Surrounded by the clouds: A comprehensive cloud reachability study," in *Proc. Web Conf.*, Ljubljana, Slovenia, Apr. 19–23, 2021, pp. 295–304.

[12] R. Mahajan, M. Zhang, L. Poole, and V. S. Pai, "Uncovering performance differences among backbone ISPs with Netdiff," in *Proc. Symp. Netw. Syst. Des. Implement.*, San Francisco, CA, USA, Apr. 16–18, 2008, pp. 205–218.

[13] H. Wu, Q. Ling, P. Mi, C. Ji, Y. Hu and Y. Pi, "Towards fine-grained, high-coverage Internet monitoring at scale," in *Proc. Asia-Pac. Worksh. Netw.*, Hong Kong, China, Jun. 29–30, 2023, pp. 130–135.

[14] J. M. D. Fiore, V. Persico, P. Mérindol, C. Pelsser, and A. Pescapé, "The art of detecting forwarding detours," *Trans. Netw. Serv. Manag.*, vol. 18, no. 3, pp. 3619–3632, Feb. 2021. doi: 10.1109/TNSM.2021.3062151.

[15] A. Alaraj, K. Bock, D. Levin, and E. Wustrow, "A global measurement of routing loops on the internet," in *Proc. Passive Act. Meas.*, Mar. 21–23, 2023, pp. 373–399.

[16] N. Gögge, E. Rohrer, and F. Tschorsch, "On the routing convergence delay in the lightning network," in *Proc. Int. Worksh. Data Priv. Manag.*, Copenhagen, Denmark, Sep. 26, 2022, pp. 203–218.

[17] J. Kucera, R. B. Basat, M. Kuka, G. Antichi, M. Yu and M. Mitzen-macher, "Detecting routing loops in the data plane," in *Proc. Int. Conf. Emerg. Netw. Exp. Tech.*, Barcelona, Spain, Dec. 01–04, 2020, pp. 466–473.

[18] P. Spadaccino, S. Bruzzese, F. Cuomo, and F. Luciani, "Analysis and emulation of BGP hijacking events," in *Proc. IEEE Symp. Netw. Oper. Manag.*, Miami, FL, USA, May 08–12, 2023, pp. 1–4.

[19] T. Holterbach, T. Alfroy, A. Phokeer, A. Dainotti, and C. Pelsser, "A system to detect forged-origin BGP hijacks," in *Proc. Symp. Netw. Syst. Des. Implement.*, Santa Clara, CA, USA, Apr. 16–18, 2024, pp. 1751–1770.

[20] O. Al-Kadi, N. Moustafa, B. P. Turnbull, and K. R. Choo, "An ontological graph identification method for improving localization of IP prefix hijacking in network systems," *Trans Inf. Forensics Secur.*, vol. 15, pp. 1164–1174, 2020. doi: 10.1109/TIFS.2019.2936975.

[21] J. Li, J. Cao, Z. Meng, R. Xie, M. Xu, "RoLL: Real-time and accurate route leak location with AS triplet features," in *Proc. Int. Conf. Commun.*, Rome, Italy, May 28–Jun. 1, 2023, pp. 5240–5246.

[22] B. A. Scott, M. N. Johnstone, P. Szewczyk, and S. Richardson, "Matrix profile data mining for BGP anomaly detection," *Comput. Netw.*, vol. 242, Feb. 2024, Art. no. 110257. doi: 10.1016/j.comnet.2024.110257.

[23] Z. Liu, H. Qiu, R. Wang, J. Zhu, and Q. Wang, "Detecting BGP anomalies based on spatio-temporal feature representation model for autonomous systems," in *Proc. Int. Conf. Trust, Sec. Priv. Comput. Commun.*, Exeter, UK, Sep. 01–03, 2023, 404–411.

[24] A. Lutu, M. Bagnulo, C. Pelsser, O. M. Maennel, and J. Cid-Sueiro, "The BGP visibility toolkit: Detecting anomalous Internet routing behavior," *Trans. Netw.*, vol. 24, no. 2, pp. 1237–1250, 2016. doi: 10.1109/TNET.2015.2413838.

[25] C. Gray *et al.*, "BGP beacons, network tomography, and bayesian computation to locate route flap damping," in *Proc. Internet Meas. Conf.*, Oct. 27–29, 2020, pp. 492–505.

[26] C. Testart and D. Clark, "A data-driven approach to understanding the state of Internet routing security," in *Proc. Res. Conf. Commun., Inform. Internet Policy*, Dec. 16, 2020.

[27] Y. Jin *et al.*, "Zooming in on wide-area latencies to a global cloud provider," in *Proc. Spec. Interest Group Data Commun.*, Beijing, China, Aug. 19–23, 2019, pp. 104–116.

[28] K. Schomp, O. Bhardwaj, E. Kurdoglu, M. Muhaimen, R. K. Sitaraman and D. N. S. Akamai, "Providing authoritative answers to the world's queries," in *Proc. Spec. Interest Group Data Commun.*, Aug. 10–14, 2020, pp. 465–478.

[29] W. B. De Vries, R. de O. Schmidt, W. Hardaker, J. Heidemann, P. -T. de Boer and A. Pras, "Broad and load-aware Anycast mapping with verfploeter," in *Proc. Internet Meas. Conf.*, London, UK, Nov. 01–03, 2017, pp. 477–488.

[30] G. C. Moura *et al.*, "Anycast vs. DDOS: Evaluating the November 2015 root DNS event," in *Proc. Internet Meas. Conf.*, Santa Monica, CA, USA, Nov. 14–16, 2016, pp. 255–270.

[31] H. V. Madhyastha *et al.*, "iPlane: An information plane for distributed services," in *Proc. Symp. Oper. Syst. Des. Implement.*, Seattle, WA, USA, Nov. 06–08, 2006, pp. 367–380.

[32] H. V. Madhyastha, E. Katz-Bassett, T. E. Anderson, A. Krishnamurthy, and A. Venkataramani, "iPlane nano: Path prediction for peer-to-peer applications," in *Proc. Symp. Netw. Syst. Des. Implement.*, Boston, MA, USA, Apr. 22–24, 2009, pp. 137–152.
[33] N. Tao, X. Chen, and X. Fu, "AS path inference: From complex network perspective," in *Proc. IFIP Netw. Conf.*, Toulouse, France, May 20–22, 2015, pp. 1–9.
[34] D. Lee, K. Jang, C. Lee, G. Iannaccone, and S. Moon, "Scalable and systematic internet-wide path and delay estimation from existing measurements," *Comput. Netw.*, vol. 55, no. 3, pp. 838–855, Feb. 2011. doi: 10.1016/j.comnet.2010.10.004.
[35] R. Nithyanand, O. Starov, P. Gill, A. Zair, and M. Schapira, "Measuring and mitigating AS-level adversaries against tor," in *Proc. Annual Netw. Distrib. Syst. Sec. Symp.*, San Diego, CA, USA, Feb. 21–24, 2016, pp. 21–24.
[36] R. Nithyanand, R. Singh, S. Cho, and P. Gill, "Holding all the ASes: Identifying and circumventing the pitfalls of AS-aware tor client design," 2016, *arXiv:1605.03596*.
[37] R. Motamedi, R. Rejaie, and W. Willinger, "A survey of techniques for Internet topology discovery," *Commun. Surv. Tutorials*, vol. 17, no. 2, pp. 1044–1065, 2015. doi: 10.1109/COMST.2014.2376520.
[38] N. E. Jerger, T. Krishna, and L. S. Peh, *Routing in On-Chip Networks*, 2nd ed. Switzerland: Springer Nature, 2017, pp. 43–56.
[39] C. Sun, Y. Ouyang, and Y. Lu, "DCBuf: A high-performance wireless network-on-chip architecture with distributed wireless interconnects and centralized buffer sharing," *Wirel Netw.*, vol. 28, no. 2, pp. 505–520, 2022. doi: 10.1007/s11276-021-02882-x.
[40] M. N. M. Ali, M. M. H. Rahman, A. A. Ibrahim, Y. Inoguchi, and E. Hossain, "The static performance effect of hybrid-hierarchical interconnection by shifted completely connected network," *IEEE Access*, vol. 9, pp. 99249–99265, 2021. doi: 10.1109/ACCESS.2021.3095146.
[41] A. Romanov, N. Myachin, and A. Sukhov, "Fault-Tolerant routing in networks-on-Chip using self-organizing routing algorithms," in *Proc. IEEE Ind. Electron. Soc.*, Toronto, ON, Canada, Oct. 13–16, 2021, pp. 1–6.
[42] S. Dill, R. Kumar, K. S. Mccurley, S. Rajagopalan, D. Sivakumar and A. Tomkins, "Self-similarity in the web," *Trans. Internet Techn.*, vol. 2, no. 2, pp. 205–223, Aug. 2002. doi: 10.1145/572326.572328.
[43] C. Song, S. Havlin, and H. Makse, "Self-similarity of complex networks," *Nature*, vol. 433, pp. 392–395, Jan. 2005. doi: 10.1038/nature03248.
[44] I. Cunha *et al.*, "Sibyl: A practical Internet route oracle," in *Proc. Symp. Netw. Syst. Des. Implement.*, Santa Clara, CA, USA, Mar. 16–18, 2016, pp. 325–344.
[45] Z. M. Mao, L. Qiu, J. Wang, and Y. Zhang, "On AS-level path inference," in *Proc. Int. Conf. Meas. Model. Comput.*, Banff, AB, Canada, Jun. 06–10, 2005, pp. 339–349.
[46] J. Qiu and L. Gao, "AS path inference by exploiting known AS paths," in *Proc. Global Telecomm. Conf.*, San Francisco, CA, USA, Nov. 27–Dec. 07, 2006, pp. 1–5.
[47] X. Y. Mu, Y. X. Chen, Y. H. Deng, and H. Zheng, "A novel algorithm for AS path inference based on BGP routing tables," in *Proc. Int. Conf. Comput. Sci. Netw. Tech.*, Tech., Dalian, China, Oct. 12–13, 2013, pp. 196–199.
[48] M. Tozal, "Policy-preferred paths in AS-level Internet topology graphs," *Theory Appl. Graph.*, vol. 5, no. 1, Mar. 2018. doi: 10.20429/tag.2018.050103.
[49] R. Singh, D. Tench, P. Gill, and A. McGregor, "PredictRoute: A network path prediction toolkit," *Meas. Anal. Comput. Syst.*, vol. 5, no. 2, pp. 23:1–23:24, Jun. 2021. doi: 10.1145/3410220.
[50] T. Wu, J. H. Wang, J. Wang, and S. Zhuang, "RouteInfer: Inferring interdomain paths by capturing ISP routing behavior diversity and generality," in *Proc. Passive Act. Meas.*, Mar. 28–30, 2022, pp. 216–244.
[51] X. Li, Z. Cai, B. Hou, N. Liu, F. Liu and J. Cheng, "ProbInfer: Probability-based AS path inference from multigraph perspective," *Comput. Netw.*, vol. 180, 2020, Art. no. 107377. doi: 10.1016/j.comnet.2020.107377.
[52] X. Li, T. Zhou, Z. Cai, and J. Su, "Realizing fine-grained inference of AS path with a generative measurable process," *Trans. Netw.*, vol. 31, no. 6, pp. 3112–3127, 2023. doi: 10.1109/TNET.2023.3270565.

[53] V. Jacobson, "Traceroute," 2006. Accessed: Aug. 21, 2024. [Online]. Available: https://wiki.geant.org/display/public/EK/VanJacobsonTraceroute#,
[54] B. Augustin *et al.*, "Avoiding traceroute anomalies with paris traceroute," in *Proc. Internet Meas. Conf.*, Rio de Janeriro, Brazil, Oct. 25–27, 2006, pp. 153–158.
[55] E. Katz-Bassett *et al.*, "Reverse traceroute," in *Proc. Symp. Netw. Syst. Des. Implement.*, San Jose, CA, USA, Apr. 28–30, 2010, pp. 219–234.
[56] K. Vermeulen, E. Gurmericliler, I. Cunha, D. Choffnes, and E. Katz-Bassett, "Internet scale reverse traceroute," in *Proc. Internet Meas. Conf.*, Nice, France, Oct. 25–27, 2022, pp. 694–715.
[57] R. Beverly, "Yarrp'ing the internet: Randomized high-speed active topology discovery," in *Proc. Internet Meas. Conf.*, Santa Monica, CA, USA, Nov. 14–16, 2016, pp. 413–420.
[58] K. Vermeulen, J. P. Rohrer, R. Beverly, O. Fourmaux, and T. Friedman, "Diamond-miner: Comprehensive discovery of the Internet's topology diamonds," in *Proc. Symp. Netw. Syst. Des. Implement.*, Santa Clara, CA, USA, Feb. 25–27, 2020, pp. 479–494.
[59] G. Huston, "Interconnection, peering and settlements," in *Proc. Internet Netw. Conf*, San Jose, Calif, Jun. 22–25, 1999, pp. 1–29.
[60] L. Gao, "On inferring autonomous system relationships in the Internet," *Trans. Netw.*, vol. 9, no. 6, pp. 733–745, 2001. doi: 10.1109/90.974527.
[61] V. Giotsas, M. Luckie, B. Huffaker, and K. Claffy, "Inferring complex AS relationships," in *Proc. Internet Meas. Conf.*, Vancouver, BC, Canada, Nov. 05–07, 2014, pp. 23–30.
[62] G. Feng, S. Seshan, and P. Steenkiste, "UNARI: An uncertainty-aware approach to AS relationships inference," in *Proc. Int. Conf. Emerg. Netw. Exp. Tech.*, Orlando, FL, USA, Dec. 09–12, 2019, pp. 272–284.
[63] Y. Jin, C. Scott, A. Dhamdhere, V. Giotsas, A. Krishnamurthy and S. Shenker, "Stable and practical AS relationship inference with Prob-link," in *Proc. Symp. Netw. Syst. Des. Implement.*, Boston, MA, USA, Feb. 26–28, 2019, pp. 581–597.
[64] Z. Jin, X. Shi, Y. Yang, X. Yin, Z. Wang, and J. Wu, "Toposcope: Recover as relationships from fragmentary observations," in *Proc. Internet Meas. Conf.*, Oct. 27–29, 2020, pp. 266–280.
[65] S. Peng, X. Shu, Z. Ruan, Z. Huang, and Q. Xuan, "Inferring multiple relationships between ASes using graph convolutional network," May 2021, *arXiv:2107.13504*.
[66] T. Shapira and Y. Shavitt, "Unveiling the type of relationship between autonomous systems using deep learning," in *Proc. Netw. Oper. Manag. Symp.*, Budapest, Hungary, Apr. 20–24, 2020, pp. 1–6.
[67] RIPE NCC, "Reseaux IP Europeens network coordination centre," Accessed: Aug. 21, 2024. 2024. [Online]. Available: https://www.ripe.net/
[68] CAIDA, "Center for applied internet data analysis," Accessed: Aug. 21, 2024. 2024. [Online]. Available: https://www.caida.org
[69] University of Oregon, "Oregon route views project," 2024, Accessed: Aug. 21, 2024. [Online]. Available: http://www.routeviews.org
[70] Princeton University, "Planetlab," 2024, Accessed: Aug. 21, 2024. [Online]. Available: https://planetlab.cs.princeton.edu
[71] Y. Xie, Z. Zhang, E. Chen, and N. Li, "AliasClassifier: A high-performance router alias classifier," *Electronics*, vol. 13, no. 9, 2024, Art. no. 1747. doi: 10.3390/electronics13091747.
[72] T. Albakour, O. Gasser, and G. Smaragdakis, "Pushing alias resolution to the limit," in *Proc. Internet Meas. Conf.*, Montreal, QC, Canada, Oct. 24–26, 2023, pp. 584–590.
[73] M. Liu *et al.*, "FBAR: An effective method for resolving large-scale IPv6 aliases," *Int. J. Commun Syst.*, vol. 36, no. 18, Sep. 2023, Art. no. e5610. doi: 10.1002/dac.5610.
[74] M. H. Gunes and K. Sarac, "Resolving IP aliases in building traceroute-based internet maps," *Trans. Netw.*, vol. 17, no. 6, pp. 1738–1751, 2009. doi: 10.1109/TNET.2009.2014227.
[75] K. Keys, Y. Hyun, M. Luckie, and K. Claffy, "Internet-scale IPv4 alias resolution with midar," *Trans. Netw.*, vol. 21, no. 2, pp. 383–399, 2013. doi: 10.1109/TNET.2012.2198887.
[76] B. Zhang, J. Bi, Y. Wang, Y. Zhang, and J. Wu, "Refining IP-to-AS mappings for AS-level traceroute," in *Proc. Int. Conf. Comput. Commun. Netw.*, Nassau, Bahamas, Jul. 30–Aug. 02, 2013, pp. 1–7.

[77] M. Luckie, A. Dhamdhere, B. Huffaker, D. Clark, and K. Claffy, "bdrmap: Inference of borders between IP networks," in *Proc. Internet Meas. Conf.*, Santa Monica, CA, USA, Nov. 14–16, 2016, pp. 381–396.
[78] A. Marder and J. M. Smith, "MAP-IT: Multipass accurate passive inferences from traceroute," in *Proc. Internet Meas. Conf.*, Santa Monica, CA, USA, Nov. 14–16, 2016, pp. 397–411.
[79] O. Darwich, H. Rimlinger, M. Dreyfus, M. Gouel, and K. Vermeulen, "Replication: Towards a publicly available internet scale IP geolocation dataset," in *Proc. Internet Meas. Conf.*, Montreal, QC, Canada, Oct. 24–26, 2023, pp. 1–15.
[80] B. Du, M. Candela, B. Huffaker, A. C. Snoeren, and K. C. Claffy, "RIPE IPmap active geolocation: Mechanism and performance evaluation," *Comput. Commun. Rev.*, vol. 50, no. 2, pp. 3–10, May 2020. doi: 10.1145/3402413.3402415.
[81] RIPE. NCC, "RIPE atlas," 2024. Accessed: Aug. 21, 2024. [Online]. Available: https://atlas.ripe.net/
[82] RIPE NCC, "Routing information service (RIS)," 2024. Accessed: Aug. 21, 2024. [Online]. Available: http://www.ripe.net/ris/
[83] CAIDA, "Archipelago (ark) measurement infrastructure," 2024. Accessed: Aug. 21, 2024. [Online]. Available: https://www.caida.org/projects/ark/
[84] CAIDA, "AS rank," 2024. Accessed: Aug. 21, 2024. [Online]. Available: http://as-rank.caida.org/
[85] T. Alfroy, T. Holterbach, T. Krenc, K. Claffy, and C. Pelsser, "Measuring internet routing from the most valuable points," in *Proc. Internet Meas. Conf.*, Nice, France, Oct. 25–27, 2022, pp. 770–771.
[86] P. Sermpezis, L. Prehn, S. Kostoglou, M. Flores, A. Vakali and E. Aben, "Bias in Internet measurement platforms," in *Proc. Netw. Traffic Meas. Anal. Conf.*, Naples, Italy, Jun. 26–29, 2023, pp. 1–10.
[87] P. Gill, M. Schapira, and S. Goldberg, "Modeling on quicksand: Dealing with the scarcity of ground truth in interdomain routing data," *Comput. Commun. Rev.*, vol. 42, no. 1, pp. 40–46, Jan. 2012. doi: 10.1145/2096149.2096155.
[88] "Isolario project," 2024, Accessed: Aug. 21, 2024. [Online]. Available: https://www.isolario.it/
[89] S. Savage *et al.*, "Detour: Informed Internet routing and transport," *IEEE Micro*, vol. 19, no. 1, pp. 50–59, Feb. 1999. doi: 10.1109/40.748796.
[90] S. Kastanakis, V. Giotsas, and N. Suri, "Understanding the confounding factors of inter-domain routing modeling," in *Proc. Internet Meas. Conf.*, Nice, France, Oct. 25–27, 2022, pp. 758–759.
[91] L. Prehn and A. Feldmann, "How biased is our validation (data) for AS relationships?," in *Proc. Internet Meas. Conf.*, Nov. 02–04, 2021, pp. 612–620.
[92] T. Green, A. Lambert, C. Pelsser, and D. Rossi, "Leveraging inter-domain stability for BGP dynamics analysis," in *Proc. Int. Conf. Passive Act. Meas.*, Berlin, Germany, Mar. 26–27, 2018, pp. 203–215.
[93] Y. Gao, W. Dong, C. Chen, X. Zhang, J. Bu and X. Liu, "Accurate per-packet delay tomography in wireless ad hoc networks," *Trans. Netw.*, vol. 25, no. 1, pp. 480–491, Feb. 2017. doi: 10.1109/TNET.2016.2594188.
[94] C. Feng, L. Wang, K. Wu, and J. Wang, "Bound inference in network performance tomography with additive metrics," *Trans. Netw.*, vol. 28, no. 4, pp. 1859–1871, Aug. 2020. doi: 10.1109/TNET.2020.3000115.
[95] H. Li, Y. Gao, W. Dong, and C. Chen, "Bound-based network tomography for inferring interesting link metrics," in *Proc. IEEE Conf. Comput. Commun.*, Toronto, ON, Canada, Jul. 06–09, 2020, pp. 1588–1597.
[96] C. Feng, J. An, K. Wu, and J. Wang, "Bound inference and reinforcement learning-based path construction in bandwidth tomography," in *Proc. IEEE Conf. Comput. Commun.*, Vancouver, BC, Canada, May 10–13, 2021, pp. 1–10.
[97] L. Ma, Z. Zhang, and M. Srivatsa, "Neural network tomography," 2020, *arXiv:2001.02942*.
[98] K. Rusek, J. Suárez-Varela, P. Almasan, P. Barlet-Ros, and A. Cabellos-Aparicio, "RouteNet: Leveraging graph neural networks for network modeling and optimization in SDN," *J. Sel. Areas Commun.*, vol. 38, no. 10, pp. 2260–2270, Aug. 2020. doi: 10.1109/JSAC.2020.3000405.
[99] Q. Zhang, K. K. W. Ng, C. Kazer, S. Yan, J. A. Sedoc and V. Liu, "MimicNet: Fast performance estimates for data center networks with machine learning," in *Proc. Spec. Interest Group Data Commun.*, Aug. 23–27, 2021, 287–304.

[100] M. Wang, L. Hui, Y. Cui, R. Liang, Z. Liu, "xNet: Improving expressiveness and granularity for network modeling with graph neural networks," in *Proc. IEEE Conf. Comput. Commun.*, London, UK, May 02–05, 2022, pp. 2028–2037.

[101] Q. Yang *et al.*, "DeepqueueNet: Towards scalable and generalized network performance estimation with packet-level visibility," in *Proc. Spec. Interest Group Data Commun.*, Amsterdam, Netherlands, Aug. 22–26, 2022, pp. 441–457.

[102] K. Zhao, P. Goyal, M. Alizadeh, and T. E. Anderson, "Scalable tail latency estimation for data center networks," in *Symp. Netw. Syst. Des. Implement.*, Boston, MA, USA, Apr. 17–19, 2023, pp. 685–702.

[103] T. B. Brown *et al.*, "Language models are few-shot learners," in *Proc. Int. Conf. Neural Inf. Process. Syst.*, Vancouver, BC, Canada, Dec. 06–12, 2020, pp. 1877–1901.

[104] L. Ouyang *et al.*, "Training language models to follow instructions with human feedback," in *Proc. Int. Conf. Neural Inf. Process. Syst.*, New Orleans, LA, USA, Nov. 28–Dec. 9, 2022, pp. 27730–27744.