Contents

Executive Summary:

Our integration of strategic measurement and analysis capabilities has enabled us to provide comprehensive annotated Internet topology maps, as well as a platform capable of Internet infrastructure assessments. We propose to research and develop new capabilities that will magnify the utility of our data mining process to specific DHS objectives. Our Applied Research Phase I will consist of three related investigations of capabilities to map router-level and AS-level topologies: how to increase their completeness; how to increase their accuracy; and how to enrich the annotations we provide.

We had inspiring success with our approach (in our BAA07-09 project) to scalable IP address alias resolution – a critical step in creating accurate router-level maps from traceroute data. Although none of the state-of-the-art tools and algorithms in this area were scalable to Internet-scale topologies, i.e., with millions of IP addresses, we extracted the most effective techniques, and re-designed, re-implemented and integrated several algorithms into a new architecture for scalable and accurate alias resolution. This approach allowed us to transfer an array of academic research related to homeland security challenges into a production resource of practical utility to DHS needs. We propose a similar technology transfer strategy with unsolved challenges in each area of investigation. To increase completeness, we will apply recently developed techniques that improve the efficiency and coverage of IP-level topology probing. To increase both completeness and accuracy, we will explore and develop additional topology data sources, and use them to improve confidence in the presence or to refute the existence of weakly observed links in our graph. To enrich our annotations, we will test and validate recently proposed techniques for creating an intermediate level of aggregation of our router-level graph, sometimes termed a “PoP-level map”. We will survey the latest work in AS relationship inference algorithms, applying and validating them as we extend our own AS-based inference algorithms to accept data path (traceroute) data as well as BGP-data as input, overcoming some of the inherent methodological problems in making inferences based on BGP data alone.

During our Development Phase II we will implement these techniques to synthesize a comprehensive Internet topology from all available data sources, as well as create support for structured queries of our topology database. In an optional phase we will demonstrate how the developed technology can support timely delivery of rich cybersecurity-relevant knowledge to DHS and fill gaps in the U.S. government’s visibility into critical cyberinfrastructure. We will contribute resulting datasets to the PREDICT repository.

The proposed work builds on CAIDA’s unique combination of strengths, capabilities, and relationships in measuring, analyzing, modeling, and visualizing Internet topology. The Ark platform has improved cybersecurity-related situational awareness of the Internet through macroscopic active measurements, including providing a more detailed and validated topological view than has ever previously been available for analysis. We have shared raw and curated forms of our resulting data with the research community to enable reproducibility and correlation with other data sources.

The resulting technologies and data will improve our ability to identify, monitor, and model critical infrastructure, specifically targeting a goal of TTA#7: “technology for the detection, prevention, and response to cyber attacks on the nation’s critical information infrastructure.”

1 Performance Goals

The Regents of the University of California; University of California, San Diego on the behalf of the San Diego Supercomputer Center's Cooperative Association for Internet Data Analysis (CAIDA) research program, offer this technical proposal which includes the following deliverables: a series of Internet Topology Data Kits (ITDK), unprecedented in cohesiveness, validation, and usability; a scalable and easy-to-use interactive interface to a database of comprehensive global Internet topology measurements; and two on-demand topology measurement tools of strategic cybersecurity relevance. To achieve these tasks, the project will extend DHS-funded Internet topology data acquisition infrastructure and Internet topology data processing, analysis, annotation, and generation software.

The proposed work targets goals outlined in TTA#7: Network Mapping and Measurement. The resulting technologies and data will improve our ability to identify, monitor, and model critical infrastructure. This project is also responsive to recommendations in the 2010 President's Council on Advisors on Science and Technology (PCAST) Report [1] which emphasizes the importance of coordinating fundamental research across DHS, DoD, and NSF on two important enablers for national and homeland security: Large-Scale Data Management and Analysis, and Cybersecurity. The proposed scope of work promises to increase our situational awareness of the Internet, support the development of new defense mechanisms for today's infrastructure, and illuminate the strengths and weaknesses in the design of the underlying architecture of our current cyber-infrastructure so that future architectures can be made truly resilient to cyber-attack, natural disaster, and inadvertent failure. Results from this project will provide valuable input for our current NSF-funded project on Future Internet Architectures [2].

2 Detailed Technical Approach

Topology maps are an important tool for those who wish to describe, analyze, and model the Internet's dynamic behavior and evolution. Several different topological layers (or granularities) are relevant to understanding the Internet as critical infrastructure, e.g., fiber, IP address, router, Points-of-Presence (PoPs), ISP (AS). Router-level and PoP-level topology maps can powerfully inform and calibrate assessments of Internet infrastructure vulnerabilities. ISP-level topologies, sometimes called AS-level or interdomain routing topologies, are critical to a deeper understanding of technical, economic, policy, and security needs of the largely unregulated peering ecosystem. Regardless of which layer of topology one seeks to map, epistemological obstacles pervade the state-of-the-art methodologies.

For example, underpinning most research into the Internet's router-level topology are data sets collected using traceroute-based algorithms. Traceroute shows the sequence of router interfaces on the path from the source to the destination, and executing traceroute from multiple sources to multiple destinations reveals many router interfaces and links, although it is possible to infer false links from this data. A critical step in creating accurate maps from traceroute data is mapping IP addresses to routers, a process known as alias resolution. A router by definition has at least two interfaces, with Internet core routers often having dozens. Alias resolution is the process of identifying which interface IP addresses belong to the same routers, which is required to convert the IP-level topology discovered by traceroute to a more useful router-level topology.

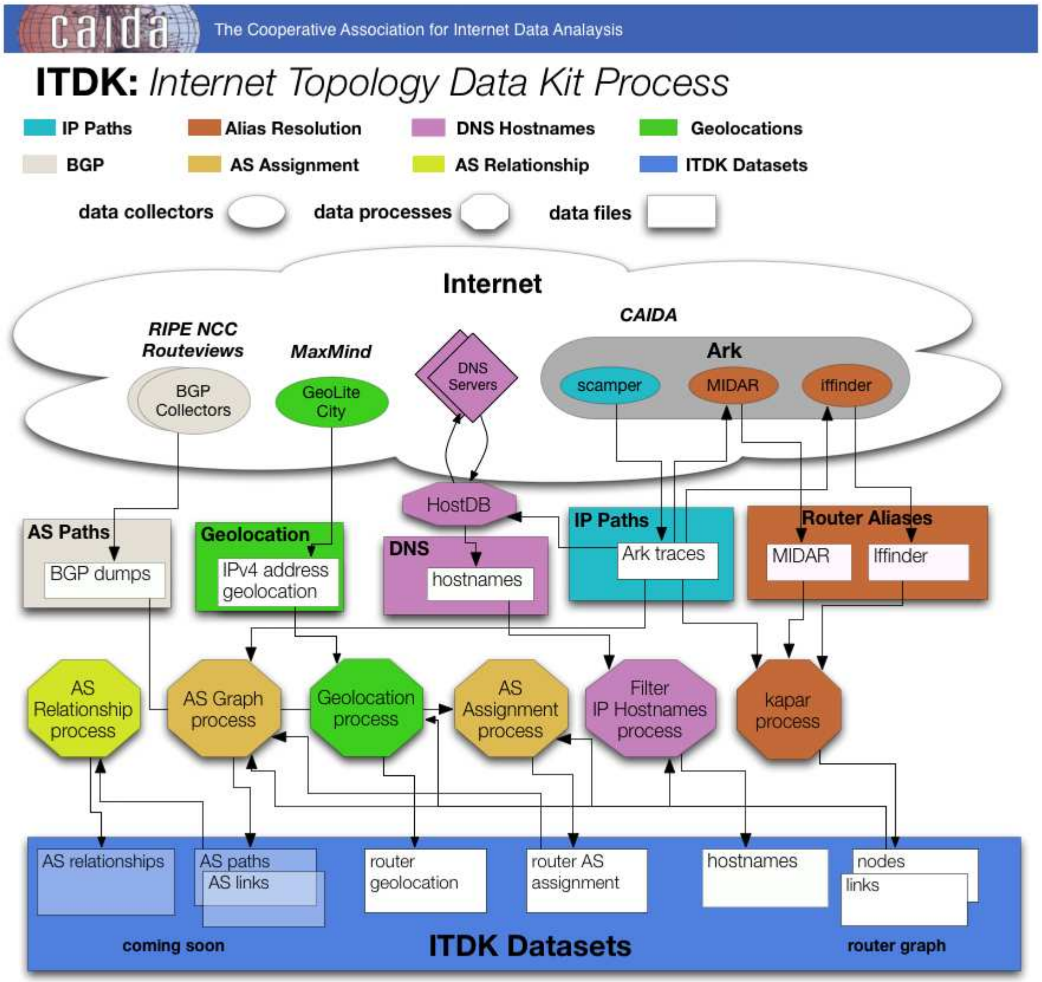


Figure 1: Internet topology data measurement, mining, and analysis process

We had inspiring success with our approach to the alias resolution problem as part of our previous (BAA07-09) mapping project. In that project we integrated (then) state-of-the-art strategic capabilities to acquire preliminary situational awareness of Internet topology structure and behavior. These capabilities included second-generation IP address alias resolution techniques and other heuristic methods to convert to IP/router and AS-level topologies, as well as limited annotation and visualization capability. Although none of the state-of-the-art tools and algorithms for alias resolution were usable with Internet-scale topologies, i.e., with millions of IP addresses, we surveyed the existing work in the area for relevance and applicability to homeland security objectives. We extracted the most effective techniques, tested and debugged them, analyzed their scalability limits, in some cases redesigning them to overcome these limits, and integrated the resulting algorithms into a new system capable of Internet-scale alias resolution with unprecedented accuracy and precision. This approach allowed us to transfer an array of relevant but preliminary academic research into a production resource of practical utility to DHS needs.

We architected a data mining and analysis process (depicted in Figure 1) for collection, curation, correlation and statistical processing of raw data on connectivity and routing gathered from a large cross-section of the global Internet, to derive a comprehensive Internet Topology Data Kit

(ITDK). Raw data sources include forward IP paths collected from traceroute-like measurement systems, BGP and geolocation information from a variety of sources, and DNS hostname information captured in parallel with topology probing. Intermediate processing involves IP address alias resolution, geolocation of routers, extraction of AS paths from BGP data, inferences of AS relationships, assignment of individual routers to ASes, and construction of an AS-level topology on top of the router-level topology to produce a dual topology. A large suite of software tools supports the collection and analysis processes.

The Ark platform has improved cybersecurity-related situational awareness of the Internet through macroscopic active measurements, including providing the most comprehensive and coherent pictures of Internet topologies to date, both at the AS- and router-level, which inspires our proposed work to take these capabilities to the next level. Data from Ark has also been used in several theoretical network science papers [3, 4, 5], including to develop a geometric framework to study the structure and function of complex networks.

Based on Ark's successful deployment of sophisticated measurement capabilities not supported by any existing infrastructure, and our successful technology transfer of academic research to solve a persistent challenge in topology analysis, we propose to research and develop new technologies and capabilities that will magnify the utility of our data mining process to support specific objectives of the Department of Homeland Security. Our Applied Research Phase I will consist of three related investigations of capabilities to map router-level and AS-level topologies: how to increase their completeness; how to increase their accuracy; and how to enrich the annotations we provide. During our Development Phase II we will implement these capabilities, as well as create support for interactive structured queries of our topology data, to address gaps in the U.S. government's current visibility into critical cyberinfrastructure. An optional Technology Demonstration Phase III will allow us to show how to use the developed technology to execute timely real-time delivery of richer cybersecurity-relevant knowledge to DHS than existing data sources have thus far been able to provide.

2.1 Applied Research Phase

Our Applied Research Phase I will consist of three related investigations of capabilities to map router-level and AS-level topologies: how to increase their completeness; how to increase their accuracy; and how to enrich the annotations we provide.

2.1.1 Task 1: Increasing the Completeness of Topologies

We will pursue several approaches to **increasing the completeness** of our data representing the Internet core: installing new monitoring infrastructure in underserved regions; integrating new techniques to improve the efficiency and coverage of IP-level topology probing; and analyzing and correlating data from Ark with other types of recently available reachability data to augment undersampled portions of the IP topology graph. These tasks will include development of software to facilitate transformation of the raw data into useful exploratory visualizations.

(a) Expand Current Monitoring Infrastructure

Funded in part by BAA07-09, Ark consists of several dozen standard PC's deployed around the world, running software that allows them to operate as a coordinated secure measurement platform

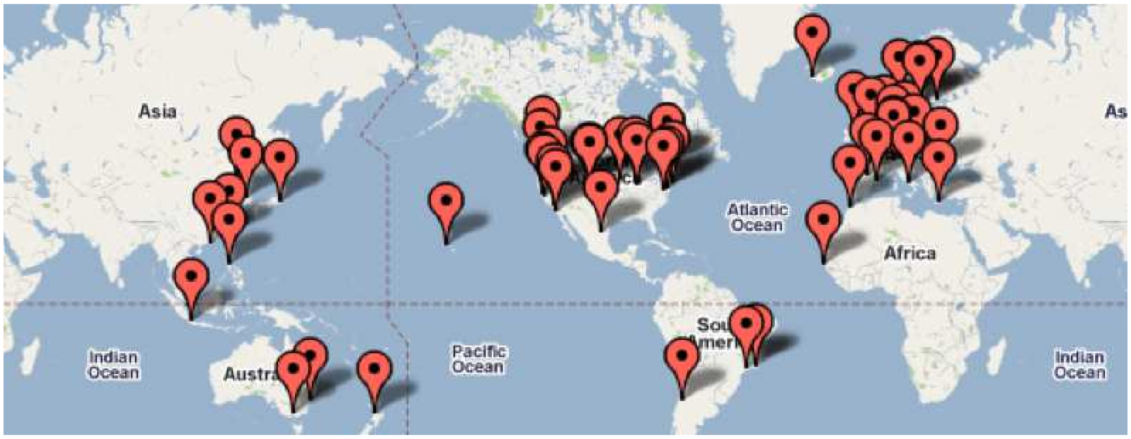


Figure 2: As of June 29, 2011 there are 54 Ark monitors in 28 countries.

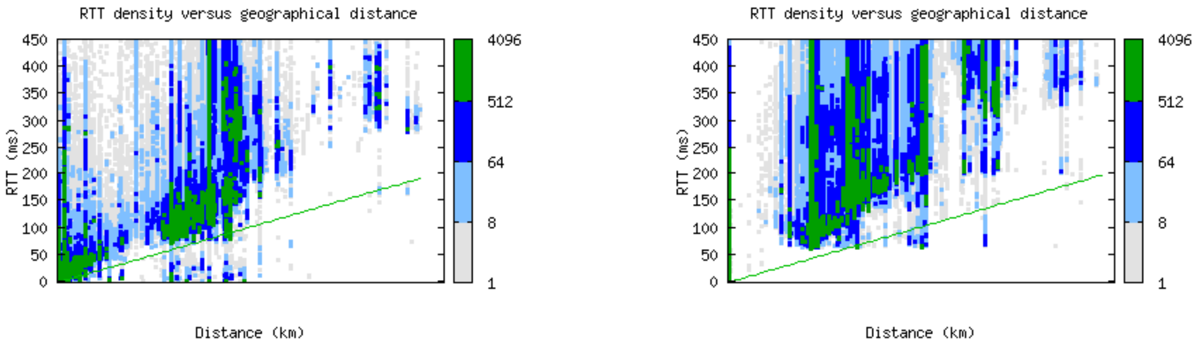
capable of performing various types of Internet infrastructure measurements and assessments. In September 2007 we began to use this novel architecture to support ongoing global Internet topology measurement and mapping. In addition to supporting strategic cybersecurity measurement experiments, Ark continuously gathers the largest set of Internet topology data for use by academic researchers.

Figure 2 depicts the 54 active Ark monitors deployed as of 1 July 2011: 20 in North America, three in South America, 19 in Europe, two in Africa, seven in Asia, and three in Oceania. We try to obtain IPv6 connectivity where available, and 27 deployed monitors have working IPv6 connectivity today. The majority of monitors are currently deployed in academic or research organizations, but recently commercial ISPs became more interested in participating. As an additional incentive for organizations to host Ark nodes, we developed a set of web pages showing per-node performance and connectivity statistics, as exemplified in Figure 3 and 4. The clustering of RTTs in Figure 3 reflects the geographic distances of the probed IP addresses from the monitor source. The Amsterdam monitor has many nearby sources, thus a large cluster of data toward the lower left of the graph, which the Dakar, Senegal monitor is fairly remote, and very few probed destinations are less than 4,000 km, or 60 ms, away. Figure 4 depicts the dispersion of AS peering interconnection near the monitor, useful for evaluating paths that data takes through upstream transit networks.

We will deploy additional monitors in geographically underserved regions, including Central America, Africa, the Middle East, India, Eastern Europe, Russia, and Southeast Asia (e.g., Cambodia, Thailand).

(b) Improve the efficiency and coverage of IP-level topology probing

To support efficient IPv4 topology measurement, Rob Beverly *et al.* developed three primitives for directed probing, Interface Set Cover (ISC), Subnet Centric Probing (SCP), and Vantage Point Spreading (VPS), that leverage external knowledge (e.g., common subnetting structures) and data from prior cycle(s) to guide the selection of probed destinations and the assignment of destinations to vantage points [6]. Such adaptive and intelligent probing is crucial to the efficiency needed for topology measurement at the scale of many millions of IP addresses. Current approaches that use a fixed subnetting boundary, e.g. probing each advertised prefix, or each /24 in IPv4, or each /48 in IPv6, are either too granular, resulting in wasted probing, or too coarse, resulting in missing information. By recursively probing destinations selected to be as distinct as possible in their most



(a) Amsterdam, NL

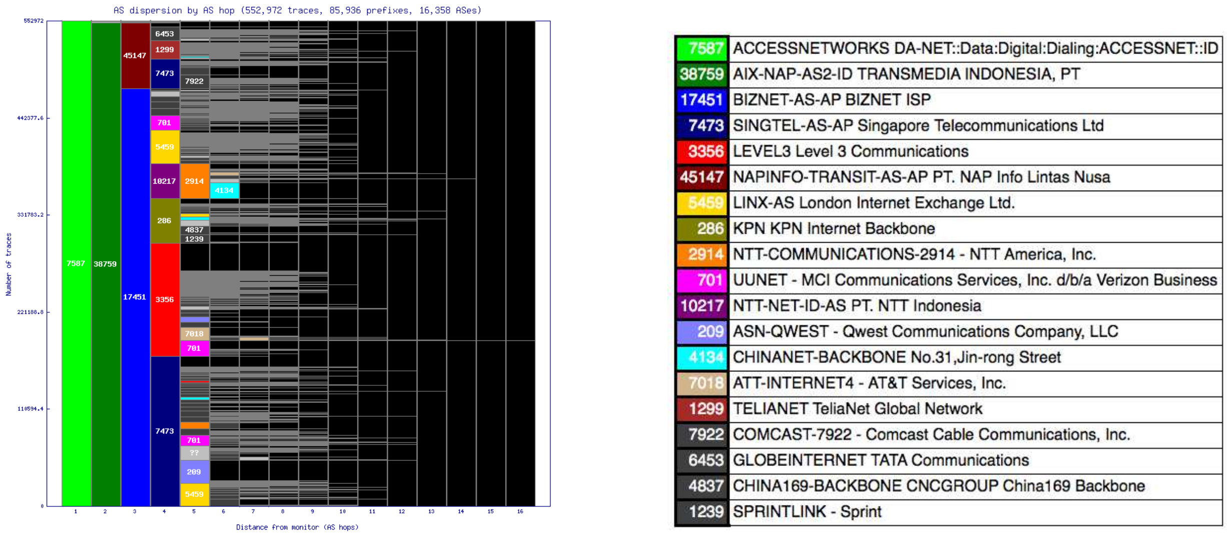
(b) Dakar, SN

Figure 3: Round-trip time (RTT) vs. geographic distance for traces to 637k destinations from two Ark nodes in Amsterdam, NL and Dakar, SN on 6 July 2011. Amsterdam's monitor has many nearby sources, thus a large cluster of data toward the lower left. Dakar's monitor is fairly remote, with few probed destinations less than 4,000 km, or 60 ms, away.

significant bits, and then examining an edit distance measure of the resulting paths, SCP is specifically designed to mitigate the granularity problem and maximally expose the internal structure of networks. Complementary to SCP is VPS which ensures maximal spreading of vantage points in order to discover path diversity leading to the destination AS. ISC generalizes prior work on adaptive probing such as DoubleTree [7] into the well-known minimum set cover problem. ISC is also multi-cycle, running across probing cycles to minimize probing while detecting load balancing and reacting to topological changes. Initial research has shown that ISC can reduce probing load by nearly 80%, thereby permitting higher-frequency probing which can reveal previously unknown dynamic and temporal properties of Internet routes. These primitives, detailed in [6], will allow us to design and implement innovations to our existing measurement architecture to support efficient large-scale topology measurement while maximizing topological fidelity.

(c) Synthesize a comprehensive Internet topology from all available sources

We will correlate IP topology data from Ark with other types of recently available topology data, including DIMES [8] and iPlane [9], to help detect reverse links and false links in our data (see Task 2), and to use as additional input for our alias resolution process. DIMES has agreed to provide full raw path information from their measurements, and intends to soon use Paris traceroute to optimize probing. The iPlane project already provides daily snapshots of their raw path information for download. We are in the process of trying to get BGP peering data from nearby the vantage points of each of our Ark monitors, which we will integrate into a locally deployed BGPMON [10] infrastructure in conjunction with directed probing to improve measurement efficiency and target probing to addresses of interest.



7587	ACCESSNETWORKS DA-NET::Data:Digital:Dialing:ACCESSNET::ID
38759	AIX-NAP-AS2-ID TRANSMEDIA INDONESIA, PT
17451	BIZNET-AS-AP BIZNET ISP
7473	SINGTEL-AS-AP Singapore Telecommunications Ltd
3356	LEVEL3 Level 3 Communications
45147	NAPINFO-TRANSIT-AS-AP PT. NAP Info Lintas Nusa
5459	LINX-AS London Internet Exchange Ltd.
286	KPN KPN Internet Backbone
2914	NTT-COMMUNICATIONS-2914 - NTT America, Inc.
701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
10217	NTT-NET-ID-AS PT. NTT Indonesia
209	ASN-QWEST - Qwest Communications Company, LLC
4134	CHINANET-BACKBONE No.31,Jin-rong Street
7018	ATT-INTERNET4 - AT&T Services, Inc.
1299	TELIANET TeliaNet Global Network
7922	COMCAST-7922 - Comcast Cable Communications, Inc.
6453	GLOBEINTERNET TATA Communications
4837	CHINA169-BACKBONE CNCGROUP China169 Backbone
1239	SPRINTLINK - Sprint

(a) AS dispersion by AS hop from Ark monitor in Indonesia

(b) AS legend for dispersion graph in (a)

Figure 4: AS peering relationships for Indonesia monitor on 6 July 2011. The most significant increase in dispersion occurs at the fourth AS hop, which based on the third AS hop appears to be a BIZNET peering point.

2.1.2 Task 2: Increasing Accuracy of Topologies

Our approach to **increasing the accuracy** of these graphs relies on a number of data sources and analysis techniques not previously available. As part of the BAA07-09 project, we demonstrated the use of Ark to perform three cybersecurity-related measurement studies of how to improve IP topology inferences: (1) assessing the quality and accuracy of various IP topology probing methods (IMC2008) [11]; (2) analyzing the prevalence and efficacy of current best practice source address validation (IP address spoofing prevention) techniques (IMC2009 [12]); and (3) evaluating the impact of one class of false links on router-level and AS-level graphs (CCR2011 [13]). We are now in a better position to explore and develop additional data sources to capture additional topology data, filter out biases and artifacts of measurement methods, and improve confidence in the presence of or refute the existence of weakly observed links in our graph. When available, we will evaluate existing technology targeting a specific problem, and transfer usable techniques into our own system, re-designing where necessary to overcome scalability limitations.

(a) Identification of false links

To inform the increasingly polarizing debate about the validity of AS links collected from different sources [14, 15, 16], we propose to investigate and mitigate the impact of false links on router-level and AS-level graphs, including identification of root causes of false link inferences e.g., load balancing, hidden nodes, stale addresses, and routing dynamics. Last year we collaborated with an external researcher to analyze the impact of one cause of false links on router-level and AS-level graphs – load-balancing – which was published in CCR 2011 [13]. Based on existing literature, we will develop techniques to quantify consensus across different sources of AS-level and traceroute data, and investigate methods to resolve knowledge conflicts among data sets, including establishing provenance of data used for inferences, and estimating the relative accuracy of data sources against as much ground truth as we can obtain. For example, seeing the same link in a number of data sources, especially if we see it in both directions, will increase our confidence in its existence. Then we will try to merge the different sources and filter out known measurement artifacts, such as load balancing effects of measurements not using Paris traceroute.

(b) Identifying AS peering relationships

Our current algorithm for inferring AS relationships (and other algorithms that have been proposed in the literature [17, 18]) assume the "no valley, prefer-customer, then prefer peer" routing policy heuristic. The no-valley assumptions include: traffic that enters a network from a provider cannot exit through another provider; traffic that enters a network from a peer cannot exit through another peer; and ISPs prefer to route traffic via customers, then peers, and use (transit) providers only as a last (most expensive) resort. Whether or not ISPs actually follow this heuristic depends on transit and peering cost structures, the nature of transit pricing contracts, and the direction of traffic for which an ISP charges its customers. Our first step in this task is to measure how often ISPs actually use the "prefer-customer, then prefer-peer" routing policy, using a combination of BGP and traceroute-based methods and ground truth AS relationship data that we are collecting as part of our AS Rank tool [19]. We will investigate observed routing anomalies to determine whether they are due to violations of the expected routing policy by the ISP, traffic engineering techniques such as selective prefix advertisements or load balancing, routing dynamics, or other factors. This analysis will inform our (and other) AS relationship algorithms that assume the validity of the "no-valley-in-BGP-path" assumption.

A further challenge in inference of peering relationships is that public repositories of BGP data [20, 21] mostly capture transit links, missing many of the pervasive (settlement-free or other) peering links. The incomplete data render it virtually impossible to accurately capture and model the complete interdomain connectivity of ASes, especially as the peering ecosystem grows increasingly diverse and resistant to simple connectivity inferences. For example, ISPs are now openly engaging in "partial peering" arrangements, i.e., peering for only a subset of routes they may announce to other providers, and explicitly block peering for other routes (prefixes), complicating and in some cases invalidating BGP-based topological inferences.

To overcome the limitations of publicly available BGP data, we have recently developed methods to ascertain the complete set of interdomain links, including peering links, for ASes that provide a BGP feed to Routeviews and RIPE RIS collectors (we call these ASes "full monitors"). To determine whether a contributing AS reveals all its links to Routeviews/RIPE (i.e., "a full peer of RouteViews/RIPE"), we use a heuristic based on comparing the number of links of X as seen directly from X with the number of links of X as seen from other Routeviews/RIPE peers, similar to the semi-global concept introduced by Broido, *et al.* in [22]. For the set of full monitors that we identify, we have developed heuristics to classify their links into transit and non-transit (settlement-free or paid peering, backup transit etc.). While we have so far applied and tested these heuristics on full monitor ASes, we will generalize these techniques to apply to other ASes. We will also investigate recently described techniques that use BGP attributes such as community and local-preference to improve AS relationship inferences [23]. Any improvements will be integrated into our production-level AS relationship inference algorithms and services, including our AS Rank tool, which ranks ASes by observable topological coverage [19]. Finally, we will extend all of our AS-level algorithms to accept data-path (traceroute) data as well as BGP-data as input, using advances made in the last several years to resolve incongruities between BGP and traceroute. This upgrade will overcome some of the inherent methodological problems in making inferences based on BGP data alone. We will document the design and implementation of this algorithm as well as our approach to usefully visualizing the data.

(c) Identifying incorrect inferences via interactive validation

Since August 2010, our deployed AS Rank tool (as-rank.caida.org) has supported interactive user validation of our AS relationship data. Lack of ground truth data has long been recognized as the greatest obstacle to improving the accuracy of topology inference and AS ranking algorithms [24, 25, 26], and we have been able to use our growing set of ground truth data [19] to improve our algorithms for identifying peering links, routers, and other annotations. We have thus far received corrections for over 1,044 peering relationships from 94 ASes. Peering inference corrections have mostly come from ASes with middle-to-high AS degrees, consistent with medium-sized ASes being more aware and interested in their position and ranking in the peering ecosystem. Tier1 ASes typically only provide general feedback, such as what percent of their neighbors were peers, providers, and customers. But they will sometimes also provide their view of their ordinal position in our AS neighbor ranking [19], which sometimes enables us to refine our peer estimation algorithm.

For this sub-task we will extend our interactive validation functionality to support interactive user corrections of AS meta-data, such as AS category (e.g., backbone, content provider, exchange point), geolocation, and organization ownership, allowing us to establish a thus far elusive public repository of AS meta-data. We will also support user-driven validation functionality for our aggregated (PoP/city)-level map inferences (see Section 2.1.3), and continue to use the gathered ground truth data to improve our inference algorithms.

2.1.3 Task 3: Enriching Annotations for Topologies

We will **enrich the annotations** on our topology maps with four types of meta-data: an intermediate level of aggregation such as infrastructure (PoP) or city location of nodes; economic data relevant to the health of the Internet ecosystem; performance (RTT) data gathered during topology probing; and confidence levels of other annotations. Where possible, we will integrate available techniques and transfer them into production, and provide a visual interface to support navigation and study of the data.

(a) Intermediate Level of Aggregation

We will provide an intermediate level of aggregation between our AS-level and router-level graph, as close to a "PoP"-level map as possible with existing technology. Two research groups have published heuristic, unvalidated approaches to construct "PoP"-level maps, i.e., mapping IP addresses to PoPs [27, 28]. We will combine these and other known techniques for making PoP-level inferences with our advanced alias resolution techniques, apply them to our topology data, and integrate the resulting PoP-level data into our bi-annual ITDK production. We will examine the possibility of using an AS's PoP-level topology to capture finer-grained AS relationships, e.g., different peering policies in different geographic regions.

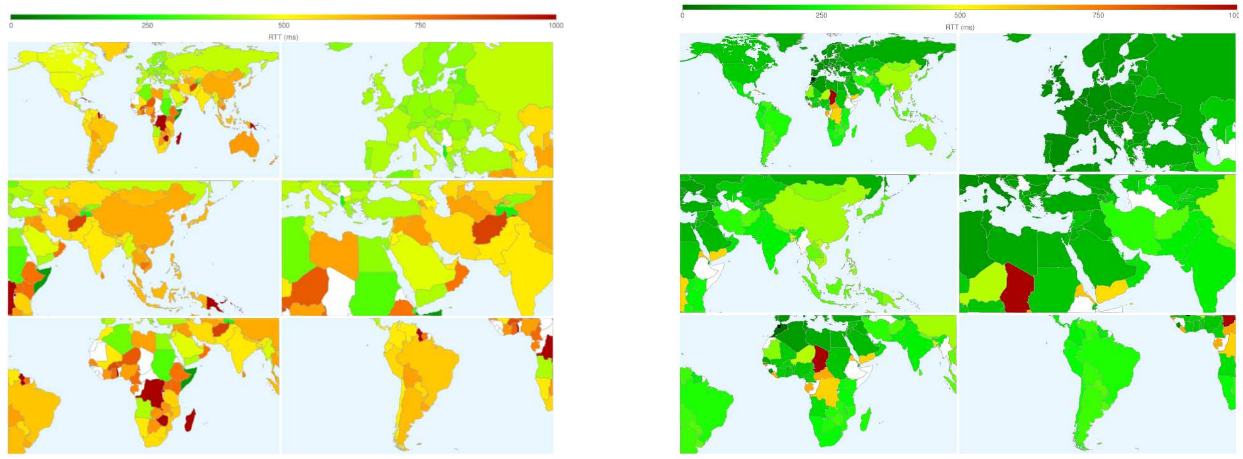
(b) Economic data relevant to infrastructure health

To enrich our AS-level economic annotations, we will extract information about ASes from peeringDB [29] snapshots which we are collecting on a daily basis. PeeringDB includes meta-data volunteered by participating networks, such as AS business type, geographic expanse (set of IXPs at which a network is present), traffic volume, and peering policy. We will use our previous AS classification scheme [30] to determine the AS type for ASes that do not participate in peeringDB. We will use technology developed in our BAA07-09 project to provide topology data at an organizational ownership granularity. Merging multiple ASes owned by a single organization into one node will be more useful for critical infrastructure analysis. Finally, we are collecting data about the financial performance of ISPs using information reported in SEC filings and other online resources. Revenue and income annotations will enable studies of the correlations between topological and economic properties of AS interconnection over time.

(c) Performance (RTT) data annotations

CAIDA has always gathered per-hop RTT data along with IP topology data – these continuous global performance measurements are probably the most underutilized component of our data. Although we provide web pages showing per-node connectivity and RTT statistics (Figure 3), we have not yet pursued historical analysis of trends or identification of RTT anomalies. Figure 3 shows a simple example of the kind of performance changes visible in two static snapshots of global RTT data from our Ark monitor in Morocco, taken before and after new cable infrastructure was installed to West Africa. Countries colored in red had the highest RTT to destinations in that country, green reflects low RTT. By 2011 Morocco had dramatically improved performance to most of the world with the exception of a few countries within Africa and the Middle East.

To make our performance data more accessible we will develop an interface to support structured querying of historical and current data (see Section 2.2), and in support of this development we will investigate techniques to identify performance anomalies as observed across monitors in different countries, e.g., RTT or reachability changes to regions of interest around the world.



(a) Median RTT per country from Moroccan Ark Monitor - 13 July 2010.

(b) Median RTT per country and state from Moroccan Ark Monitor - 6 July 2011.

Figure 5: The median RTT per country shown from the Ark monitor located in Casablanca, Morocco approximately one year ago. We believe the drastic reduction in RTTs from this monitor comes from new cable infrastructure recently connected to West Africa [31].

2.2 Development Phase

Our development phase includes three main deliverables: (1) release two Internet Topology Data Kits per year; (2) develop a user-friendly interactive visual interface to topology data and meta-data; and (3) implement two on-demand topology measurement tools.

2.2.1 Task 1: Internet Topology Data Kits

We make several curated data sets (observed router-level topology, AS-links, AS relationships) available as “soft infrastructure” to researchers to enable reproducibility and correlation with other data sources. As of July 2011, CAIDA has vetted 557 user accounts for access to our ITDK and other topology datasets. We will put into production a single cohesive “canonical data set” that combines all the data and meta-data that we will provide: raw traceroute data; router-level topologies; geographic location of each router; infrastructure-level (PoP, if possible) information; router-to-AS assignments; DNS lookups of observed addresses; AS peering relationships; and economic data relevant to infrastructure health. We will contribute these canonical data sets to the PREDICT repository.

2.2.2 Task 2: Interactive visualization and query interface to topology data

We will develop new visualization software to make the above data sets more operationally useful. We will support a coupled, rather than the current independent, visualizations of AS-level and router-level graphs, and depict ownership structure, business relationships, geographic coverage, and financial indicators. Joint visualizations of topological and economic metrics can be used to study the economic health and diversity of the Internet ecosystem over time.

To make our accumulated topology data easier for others to use, we will create interactive support for structured queries of our topology data, using information visualization techniques to present results. We will support interactive queries regarding observable reachability and performance changes and trends from, to, and across specific regions of the world, addressing gaps in the U.S. government’s current visibility into critical cyberinfrastructure. We will create a user-friendly graphical user interface whereby a DHS-appointed official could request to view existing measurement results, such as “Show me all connectivity statistics from all monitors to all addresses that geolocate to Egypt, Libya, and Algeria.” This new functionality will allow the user to examine historical and current data from selected monitors to probed destinations by country, AS, BGP prefix, or organization. This interface will allow user corrections of false inferences, which we will then validate by email.

2.2.3 Task 3: On-demand topology measurement tools

We will build two tools that showcase the progress we have made on infrastructure development and topology data analysis. First, we will develop *topo-on-demand*, which allows a user to request the Ark platform to perform a limited set of reachability measurements from and to a user-specified set of hosts in real time. A user-friendly graphical user interface (GUI) will enable selection of probing destinations by country, AS, BGP prefix, or organization. Such focused measurements can be used, for example, to observe the unreachability of an entire geographic region.

Second, we will build on the progress made on router annotations in the last several years [32] to build a publicly available AS-level traceroute tool. Attempts have been made in the past to build such a tool [33] but were blocked on accurate AS-level inferences of router ownership, and were never made public. We will refine the algorithms in [33] with new techniques to adjust IP-to-AS mappings derived from traceroute. We will report the best estimate for the primary AS-level path to a given destination in real-time, annotated with confidence levels for inferences. Such a tool is directly responsive to the call in TTA#7 for "technology for the detection, prevention, and response to cyber attacks on the nation's critical information infrastructure. [34]"

2.3 Technology Demonstration Phase

An optional Technology Demonstration Phase III will allow us to show how to use the developed technology to execute timely real-time delivery of richer cybersecurity-relevant knowledge to DHS than existing data sources have thus far been able to provide. Each instance of our Internet Topology Data Kit demonstrates how the technology developed in our Applied Research Phase can create a useful data source with clear provenance for use by researchers and critical infrastructure analysts. We will demonstrate the user-friendly structured query interface to our historical database of topology measurements, and visualizations of macroscopic reachability changes from Ark nodes to specific destinations, such as the unreachability of an entire geographic region. Finally, we will demonstrate the new functionality in our AS Ranking tool.

3 Testing and Evaluation

Our tests come in the form of large scale measurement experiments run on the Archipelago Measurement (Ark) Infrastructure. CAIDA tailored Ark specifically for Internet-scale active probing experiments. As an example of our testing environment, each complete execution of our MIDAR system [35] to support scalable alias resolution requires four stages of measurement and analysis to construct a router-level graph. The stages of test execution include Estimation, Discovery, Elimination, and Corroboration. In the *Estimation* stage, we determine the velocity and best probe method for each address for use in subsequent stages. In the *Discovery* stage, we probe all target addresses with a sliding window schedule that allows us to efficiently discover pairs that potentially share an IP ID counter. In the *Elimination* stage, we re-probe the potential alias pairs to rule out most false positives. Finally, in the *Corroboration* stage, we probe each candidate alias set as a whole to confirm them and to rule out remaining false positives. After completion of all probing stages, we infer reliable alias sets using all available data and results.

With each run we create a new Internet Topology Data Kit (ITDK) [36], which synthesizes measurement and analysis efforts into a comprehensive view of Internet connectivity at multiple granularity levels, including the router-level graph. We evaluate the resulting data using standard statistical methods as well as with *topostats*, a package of programs that calculate various statistics on network topologies (graphs) [37]. This tool suite currently calculates and reports statistics on: node and edge count, degree statistics of nodes and neighbors, assortativity, clustering, coreness, path distances, eccentricity, radius, and betweenness. Unfortunately it does not yet work on hypergraphs and multigraphs, which are more faithful representations of Internet interconnection topology. To support evaluation of consistency and trends across ITDKs, we will extend this topology statistics analysis software library [37] to work on hypergraphs and multigraphs.

Security and network researchers using ITDK datasets are inevitably testing and evaluating their utility for scientific research [38, 39, 40, 41, 42, 43]. CAIDA receives dozens of researcher requests monthly for access to data. As of July 1, 2011, CAIDA has vetted 557 user accounts for access to our ITDK and other topology datasets. These users conduct research and publish in various fields of study including traffic analysis, compact routing, graph and field theory, complex networks, topology evolution and economics and more recently censorship and international policy analysis.

4 Commercialization Plan

CAIDA made previous attempts in licensing software technologies to commercial spinoffs, but the licenses were eventually returned to UCSD and not further developed because of the lack of designated funding. CAIDA embraces open source software licenses as an appropriate channel to transfer the results of our research and development effort to benefit the public and the nation. We will make software tools from this project available with an open source license (e.g., GPL) consistent with university policy.

CAIDA regularly communicates with Internet-related companies to exchange research and operational expertise and organizes regular workshops that are internationally renowned for bringing together Internet researchers, operators, and policy makers.

Finally, CAIDA is an active participant in the PREDICT repository project. We will continue to use PREDICT to share the collected topology data with vetted researchers. CAIDA actively promotes technology transfer of methods and data to the research community. Through our membership program, we make our technology and data available to industrial partners. To date, academic researchers account for approximately 90% of downloads and commercial and government researchers make up the remaining 10%. As of June 1 2011, our topology datasets (collected using Ark) have grown to over 4.5+ terabytes.

5 Facilities

A general description of SDSC/UCSD and CAIDA facilities and equipment follows. The Cooperative Association for Internet Data Analysis (CAIDA) is housed in the San Diego Supercomputer Center (SDSC) building on the UCSD campus. UCSD provides sufficient office space for the entire team as well as telephones, photocopying resources and computer networks. The available physical space accommodates all essential facilities for the proposed project: conference rooms, teleconferencing facilities for interaction with other industrial and academic researchers, and high-bandwidth networking. SDSC maintains connectivity to the Internet via multiple 10GE upstream connections via fiber optic network.

CAIDA facilities and equipment hosted at SDSC include enterprise desktops, laptops, and numerous dedicated servers for computational analysis and visualization, data curation, storage and distribution. CAIDA develops and maintains remote Archipelago measurement infrastructure tailored specifically for active probing experiments.

The resources available through SDSC include supercomputers, archival storage systems, data-handling platforms, and advanced visualization systems. The center continually upgrades its facilities to provide a robust environment for cyberinfrastructure research, development and deployment.

The modern, energy-efficient data center at SDSC was expanded in 2009 to allow more floor space, power, and cooling capacity for the computational resources as needed by this project and others. Data-handling resources include a storage-area network (SAN) with multi-petabyte capabilities for storage and archival. SDSC's data-handling environment provides support for databases, data management, and data mining. Associated data-intensive computing software includes the Storage Resource Broker, a distributed data-handling system developed at SDSC, digital library technology acquired through collaborations with MIT and Cornell, parallel object-relational database technology acquired in collaboration with IBM, and the Data Oasis Cloud and archival storage system currently under development and testing. SDSC has integrated these systems to provide support for massive data collections.

The SDSC Synthesis Center enables collaborative viewing of scientific data and advanced scientific visualization capabilities. A complete video and audio production suite is used to produce publication quality animations. The video lab is network accessible and can be used to render scientific images.

SDSC has a staff of more than 200 scientists, software developers, and support personnel and plays a leading role in several major data projects for various disciplines including seismology, neuroscience, molecular science, Earth systems science, and astronomy. Access to these data collections is provided through the SDSC Storage Resource Broker. The combination of information management technology, scientific data collections, and the rapid access data-handling platforms creates an excellent testbed for evaluating new approaches to managing scientific data and scientific algorithms.

The IT support infrastructure at SDSC provides 24/7 production level support and working day (8/5) help desk/user services support to assist in resolving technical issues. This project will make use of the full expertise and institutional SDSC experience as necessary.

6 Government-Furnished Resources

Data and software distribution resulting from this work will make use of the framework and resources of the Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT) supported by the DHS. Our datasets will be available to other researchers for studies on cyber security via PREDICT. When appropriate, we will use data available from the PREDICT repository for corroboration and cross-correlation with our measurement results.

To accomplish the proposed work, we need to expand our measurement infrastructure Ark into currently underrepresented areas. We also need to maintain Ark's functionality and to replace obsolete or failing monitors. We request funds for 20 Ark monitors, at an approximate cost of $750 each, to be purchased as Contractor Acquired Property.

Contractor Acquired Property will include three laptops to be used by the Senior Personnel for project related tasks and while traveling.

References

[1] Executive Office of the President and Presidents Council of Advisors on Science and Technology, "Report to the President and Congress Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology," 2010. `http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf`.

[2] "Named Data Networking Research Project," 2010. `http://named-data.net/`.

[3] M. Boguñá and D. Krioukov, "Navigating Ultrasmall Worlds in Ultrashort Time," *Phys. Rev. Lett.*, vol. 102, p. 058701, Feb 2009.

[4] M. Boguñá, F. Papadopoulos, and D. V. Krioukov, "Sustaining the Internet with Hyperbolic Mapping," *CoRR*, vol. abs/1009.0267, 2010.

[5] M. A. Serrano, D. Krioukov, and M. Boguñá, "Percolation in Self-similar Networks," *Phys. Rev. Lett.*, vol. 106, p. 048701, Jan 2011.

[6] R. Beverly and A. Berger and Geoffrey G. Xie, "Primitives for Active Internet Topology Mapping: Toward High-Frequency Characterization," *Proceedings of the ACM SIGCOMM conference on Internet Measurement*, November 2010.

[7] B. Donnet, P. Raoult, T. Friedman, and M. Crovella, "Efficient Algorithms for Large-scale Topology Discovery," in *Proceedings of the 2005 ACM SIGMETRICS*, 2005.

[8] Y. Shavitt and E. Shir, "DIMES: Let the Internet Measure Itself," *SIGCOMM Comput. Commun. Rev.*, vol. 35, pp. 71–74, October 2005.

[9] Harsha V. Madhyastha and Ethan Katz-Bassett and Tom Anderson and Arvind Krishnamurthy and Arun Venkataramani, "iPlane: An Information Plane for Distributed Services." `http://iplane.cs.washington.edu/`.

[10] "BGP Monitoring System: Next Generation Software Dedicated to BGP Monitoring," July 2009. `http://bgpmon.netsec.colostate.edu`.

[11] M. Luckie, Y. Hyun, and B. Huffaker, "Traceroute Probe Method and Forward IP Path Inference," in *Internet Measurement Conference 2008*, Oct 2008.

[12] R. Beverly, A. Berger, Y. Hyun, and K. Claffy, "Understanding the Efficacy of Deployed Internet Source Address Validation Filtering," in *8th Internet Measurement Conference (IMC)*, November 2009.

[13] M. Luckie, A. Dhamdhere, K. Claffy, and D. Murrell, "Measured Impact of Crooked Traceroute," *ACM Computer Communications Review*, January 2011.

[14] Y. Zhang, R. Oliveira, H. Zhang, and L. Zhang, "Quantifying the Pitfalls of Traceroute in AS Connectivity Inference," in *Proceedings of the 11th international conference on Passive and active measurement*, Proceedings of the 2010 Passive and Active Measurement Workshop, 2010.

[15] Z. M. Mao, L. Qiu, J. Wang, and Y. Zhang, "On AS-level Path Inference," in *Proceedings of ACM SIGMETRICS*, (New York, NY, USA), pp. 339–349, ACM, 2005.

[16] Willinger, Walter and Alderson, David, and Doyle, John C., "Mathematics and the Internet: A Source of Enormous Confusion and Great Potential," *American Mathematical Society*, vol. 56, no. 5, 2009.

[17] Lixin Gao, "On Inferring Autonomous System Relationships in the Internet," *IEEE ACM Transactions on Networking*, vol. 9, Dec 2001.

[18] X. Dimitropoulos, D. Krioukov, M. Fomenkov, B. Huffaker, Y. Hyun, and G. Claffy, K. Riley, "AS Relationships: Inference and Validation," in *ACM SIGCOMM Computer Communications Review*, 2007.

[19] CAIDA, "Ranking of Internet Service Providers by Observed Topology," 2010. `http://as-rank.caida.org/`.

[20] Routeviews, "University of Oregon Route Views Project." `http://www.routeviews.org`.

[21] RIPE, "RIS Raw Data." `http://www.ripe.net/data-tools/stats/ris/ris-raw-data`.

[22] A. Broido, E. Nemeth, and K. Claffy, "Internet Expansion, Refinement, and Churn," *European Transactions on Telecommunications*, vol. 13, no. 1, pp. 33–51, 2002.

[23] V. Giotsas and S. Zhou, "Inferring AS Relationships from BGP Attributes," *arxiv*, 2011.

[24] kc claffy, M. Fomenkov, E. Katz-Bassett, R. Beverly, B.Cox, and M. Luckie, "The Workshop on Active Internet Measurements (AIMS) Report," *Computer Communication Review*, vol. 39, no. 5, 2009.

[25] kc claffy, E. Aben, J. Augé, R. Beverly, F. Bustamante, B. Donnet, T. Friedman, M. Fomenkov, P. Haga, M. Luckie, and Y. Shavitt, "ISMA 2010 AIMS-2 - Workshop on Active Internet Measurements Report," *Computer Communication Review*, vol. 40, no. 5, 2010.

[26] kc claffy, "ISMA 2011 AIMS-3 - Workshop on Active Internet Measurements Report," *Computer Communication Review*, vol. 41, no. 3, 2011.

[27] Madhyastha, Bassett, Anderson, Krishnamurthy, Venkataramani, "iPlane Nano: Path Prediction for Peer-to-peer Applications," *USENIX Networked Systems Design and Implementation conference*, 2009.

[28] Y. Shavitt and N. Zilberman, “A Structural Approach for PoP GeoLocation,” *Proceedings of the 2010 IEEE INFOCOM Conference*, 2010.

[29] “Peeringdb peering database.” `http://www.peeringdb.com`.

[30] A. Dhamdhere and C. Dovrolis, “Twelve Years in the Evolution of the Internet Ecosystem,” *IEEE/ACM Transactions on Networking*, vol. PP, March 2011.

[31] T. Maliti, “New Cables Tie West Africa Closer to Internet,” Sep 2010. `http://www.msnbc.msn.com/id/38886073/ns/technology_and_science-tech_and_gadgets/t/new-cables-tie-west-africa-closer-internet/`.

[32] Huffaker, Bradley and Dhamdhere, Amogh and Fomenkov, Marina and claffy, kc, “Toward Topology Dualism: Improving the Accuracy of AS Annotations for Routers,” *Lecture Notes in Computer Science*, vol. 6032, April 2010. `http://www.caida.org/publications/papers/2010/as_assignment/`.

[33] Z. Mao, D. Johnson, J. Rexford, J. Wang, and R. Katz, “Scalable and Accurate Identification of AS-level Forwarding Paths,” in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 3, march 2004.

[34] Department of Homeland Security, “Cyber Security Research And Development Broad Agency Announcement BAA 11-02,” February 2012. `https://www.fbo.gov/index?s=opportunity&mode=form&id=40161dd972cd60642ecaaa955e247067`.

[35] K. Keys, Y. Hyun, M. Luckie, and k claffy, “CAIDA Internet-Scale IPv4 Alias Resolution with MIDAR: System Architecture - Technical Report,” May 2011. `http://www.caida.org/publications/papers/2011/midar-tr/midar-tr.pdf`.

[36] “CAIDA Macroscopic Internet Topology Data Kit (ITDK).” `http://www.caida.org/data/active/internet-topology-data-kit/`.

[37] Ryan Koga and Young Hyun, “Topology Statistics Analysis Tool,” 2010. `http://www.caida.org/tools/utilities/topostats/`.

[38] S. D. Strowes, G. Mooney, and C. Perkins, “Compact Routing on the Internet AS-graph,” in *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*, april 2011.

[39] Tomasik, J. and Weisser, M.-A., “Internet Topology on AS-level: Model, Generation Methods and Tool,” in *Performance Computing and Communications Conference (IPCCC), 2010 IEEE 29th International*, Dec. 2010.

[40] J. Scholz and M. Greiner, “Self-organizing Weights for Internet AS-graphs and Surprisingly Simple Routing Metrics,” *Europhysics Letters (EPL)*, vol. 94, no. 2, 2011.

[41] D. Huang, J. Zhao, and X. Wang, “Trading Bandwidth for Playback Lag: Can Active Peers Help?,” in *Proceedings of the international conference on Multimedia*, MM ’10, (New York, NY, USA), pp. 791–794, ACM, 2010.

[42] H. Asai and H. Esaki, “Estimating AS Relationships for Application-Layer Traffic Optimization,” in *Incentives, Overlays, and Economic Traffic Control* (B. Stiller, T. Hofeld, and G. Stamoulis, eds.), vol. 6236 of *Lecture Notes in Computer Science*, pp. 51–63, Springer Berlin / Heidelberg, 2010.

[43] S. Shakkottai, M. Fomenkov, R. Koga, D. Krioukov, and K. C. Claffy, “Evolution of the Internet AS-level Ecosystem,” *The European Physical Journal B - Condensed Matter and Complex Systems*, vol. 74, pp. 271–278, 2010. 10.1140/epjb/e2010-00057-x.

A Assertion of Data Rights

Data and software resulting from this work make use of the framework previously established by the DHS PREDICT project.

The offeror asserts for itself, or the persons identified below, that the Government's rights to access, use, modify, reproduce, release, perform, display, or disclose only the following technical data or computer software should be restricted.

The offerer has reviewed the requirements for the delivery of data or software and states:

Data proposed for fulfilling such requirements qualify as limited rights data or restricted computer software and are identified as follows:

1. IPv4 topology data collected on Ark platform
2. IPv6 topology data collected on Ark platform
3. Data for IP-to-router resolution (derived)
4. Ark-based router-level topologies and graphs (derived)
5. Geographic locations of each router and DNS lookups of all observed IP addresses
6. Ark-based AS-level topologies and graphs (derived)
7. Ark-based annotated dual AS-router topologies and graphs (derived)

These data come with limited distribution rights as they contain IP addresses that may be used to reveal details about end users including names, geographic and network location, organization, and other personal and private information and should not be subject to unauthorized access. Except for the above, the Offeror (UCSD) can provide the government with unlimited rights for government purposes regarding this proposal.