

Internet Atlas: A Geographic Database of the Internet

Ramakrishnan Durairajan
University of
Wisconsin-Madison
rkrish@cs.wisc.edu

Subhadip Ghosh
University of
Wisconsin-Madison
sghosh@cs.wisc.edu

Xin Tang
University of
Wisconsin-Madison
xtang@cs.wisc.edu

Paul Barford
University of
Wisconsin-Madison
pb@cs.wisc.edu

Brian Eriksson
Technicolor Research
brian.eriksson@technicolor.com

ABSTRACT

This paper describes *Internet Atlas*, a new visualization and analysis portal for diverse Internet measurement data. The starting point for Atlas is a geographically anchored representation of the *physical Internet* including (i) nodes (e.g., hosting facilities and data centers), (ii) conduits/links that connect these nodes, and (iii) relevant meta data (e.g., source provenance). This physical representation is built by using search to identify primary source data such as maps and other repositories of service provider network information. This data is then carefully entered into the database using a combination of manual and automated processes including consistency checks and methods for geocoding both node and link data. Atlas currently contains over 9.5K PoP locations and nearly 13.5K links for over 270 networks around the world. Customized interfaces were built to import a variety of dynamic (e.g., BGP updates, Twitter feeds and weather updates) and static (e.g., highway, rail and census) data into Atlas, and to layer it on top of the physical representation. The openly available web portal [15] is based on the widely-used ArcGIS geographic information system [19], which enables visualization and diverse spatial analyses of the data. We describe the details of the portal implementation as well as on-going efforts to expand its capabilities.

Categories and Subject Descriptors: C.2.1 [Network Architecture and Design]: Network topology C.2.3 [Network Operations]: Public networks H.2.8 [Database Applications]: Spatial databases and GIS

Keywords: Internet topology; Internet maps; physical network connectivity; geographic database

1. INTRODUCTION

Accurate and timely maps of the Internet would provide a starting point for diverse research topics such as assessing

infrastructure vulnerabilities, understanding routing behavior, developing new protocols, analyzing application performance, and large scale network simulation studies. Such maps would also be highly valuable in network operations since they could provide insights to fault diagnosis, opportunities for peering and transit, and planning for future growth. However, despite the many and varied efforts over the years, there remains no central repository of accurate Internet maps.

The lack of a central repository of Internet maps can be attributed to several significant challenges. First, it is well known that the Internet is a gigantic and complex worldwide infrastructure that is in a constant state of flux. Second, the fundamental “network-of-networks” organization of the Internet means that no single provider can offer an authoritative perspective on structure. Third, the de facto use of IP addresses gathered from TTL-limited probing campaigns as the basis for inferring structure has inherent difficulties. These include the well known interface disambiguation problem [26], widely varying policies on probe blocking among providers, and difficulties in managing large scale measurement infrastructures [24]. We believe that a different approach to building and maintaining a repository of Internet maps is required.

In this paper, we describe the *Internet Atlas* project. Our objective is to build a comprehensive, geographically accurate map of the physical Internet *i.e.*, nodes (e.g., hosting facilities and data centers) and links (e.g., optical fiber conduits), extend this map with relevant, related data (e.g., BGP updates, etc.), and to make the data available through a web portal for visualization and analysis. We posit that such an infrastructure would lend itself directly to a wide range of research and operational applications that have motivated prior Internet mapping efforts.

Our first focus is on developing a comprehensive and geographically accurate representation of the Internet’s *physical interconnection structure*. Specifically, we seek to identify the locations of the buildings that house switching and routing equipment as well as the paths of physical conduits that connect them. We argue that this physical perspective is (i) likely to be a much smaller graph than those produced from layer 3 measurements, thus potentially making the mapping process more tractable, (ii) likely to change over much longer time scales, again making the mapping process more tractable, and (iii) a foundation for understanding other Internet-related measurements.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

HotPlanet’13, August 16, 2013, Hong Kong, China.

Copyright 2013 ACM 978-1-4503-2177-8/13/08 ...\$15.00.

To produce a comprehensive map of the physical Internet we use search to identify infrastructure maps and other repositories that are published online by service providers. Unfortunately, the maps that are identified have no consistent format – some are images, others are embedded in Flash applications and all are given with a variety of geographic details. Geographic accuracy is aided by the fact that many service providers list street addresses of the locations of their PoPs, and listings of the same street addresses from multiple service providers (indicating a third party hosting facility) increases confidence in the overall map. Some of our data collection and entry process are automated, however others must still be done by hand (*e.g.*, verification). The current Atlas repository includes 9,677 PoP locations and 13,820 links for 279 networks (including all tier-1 providers) around the world. A snapshot of the Atlas portal showing all the identified PoPs can be seen in Figure 1. Published maps of service provider networks are periodically checked for updates, and new maps are being added to the repository on an on-going basis.

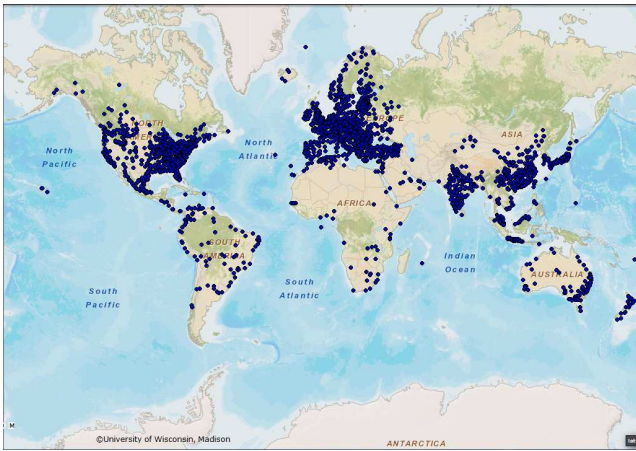


Figure 1: Map of the locations of Points of Presence that are currently available in Internet Atlas.

Our second focus is to use the representation of the physical Internet as the starting point for assembling and associating additional data types. Specifically, we seek to use geographic anchors to tie together diverse data types including Internet measurements, social media, public infrastructure, weather reports, *etc.* We argue that this combined representation offers a unique perspective and opportunity to address a broad set of research and operational problems. We have implemented a variety of interface mechanisms that enable diverse data to be automatically pulled into the Atlas repository. The current Atlas repository includes BGP updates, weather service, hurricane and earthquake data, Twitter feeds, US census data, Dshield attack data, US highway and rail maps. Additional data types are being added on an on-going basis.

The Atlas repository is implemented on top of the widely-used Geographic Information System, ArcGIS [19], which includes an object-relational database that is purpose-built for data that is geographically organized. This design choice was motivated by the robust visualization and geo-analytic capabilities that are available in ArcGIS, the availability of a large number of third party geo-coded databases (*e.g.*, census and infrastructure data), and our desire to be able

to flexibly overlay and analyze multiple data types on top of our physical Internet representation.

Our third focus is to enhance the utility and flexibility of the repository through a public web portal. Beyond the interface to ArcGIS, requirements for the portal include broad compatibility, high performance, ease-of-use, extensibility, security, auditing, and user based access control. To satisfy these requirements the portal is implemented in Java using the Spring Framework [13]. We also use Adobe’s Flex SDK [16] to build rich, dynamic applications on top of the ArcGIS server. The portal enables users to visualize all of the data in a layered fashion, browse the repository, search the repository, flexibly organize and display aggregates of networks over base maps of the earth. Similar to the repository, the new capabilities are being added to the portal on an on-going basis. The current version of the portal is openly available to the community at [15].

2. RELATED WORK

Analyzing the interconnection structure of the Internet has been the subject of a large number of studies over the past decade. The network scope of these studies range from the router-level (*e.g.*, [17, 22]), to PoP-level (*e.g.*, [25, 26]), to the autonomous system-level (*e.g.*, [29, 23]). Most of these studies are based on layer 3 measurements from *traceroute*-like tools at the router-level, and BGP announcements at the AS level (*e.g.*, [10]). The dynamic nature of the data used in these studies presents significant challenges in recovering details of the underlying physical infrastructure. Internet Atlas differs significantly from these studies in overall objectives and the fact that it uses network maps from service providers as the basis for building a larger map of the physical Internet.

The study that bears the strongest resemblance to ours is the Internet Topology Zoo [21], which offers representations of service provider maps that are discovered from search (Gorman used a similar approach in his Ph.D. thesis [20] although no maps from that work are available). Indeed, we used the Topology Zoo as a source of data for our repository. However, Internet Atlas goes well beyond Topology Zoo by including: (1) Dynamic, GIS-based visualization including search, filtering and overlaying of multiple networks, (2) A larger and more diverse repository of network node locations, (3) Real-time data feeds (*e.g.*, BGPmon and NOAA weather reports) layered on top of maps of physical infrastructure, (4) Static geo-coded data (*e.g.*, census and infrastructure), (5) Geo-location of physical links (when available from maps) and (6) Geo-spatial analyses (*e.g.*, Kriging estimation). To the best of our knowledge, Internet Atlas is the first academic effort to establish a GIS-based web portal that includes diverse measurement data layers on top of a map of the physical Internet.

3. INTERNET ATLAS DATA REPOSITORY

In this section, we describe the processes and tools that were developed to build and maintain the Atlas repository.

3.1 Identifying Network Data Sources

Internet Atlas is predicated on the assumption that detailed information on network infrastructure can be found

on publicly available webpages.¹ This implies that Internet search can be used as the primary data gathering tool. In addition to the major search engines, we used search aggregators, such as Soovle [12] and SidePad [11] to enhance the ability to find network maps.

Our search objective is to find any and all maps/listings of Internet infrastructure. Several important lessons were learned through extensive trial-and-error exploration of relevant search terms. For example, simple one-word terms, such as “co-location” or “datacenter”, resulted in discovery of very few previously unseen networks/locations, while multiple word phrases, such as “co-location facility” or “telecom hotels” were more productive.² The most important lesson learned is that geographic specificity in search terms is extremely important in revealing regional and local providers. While this may seem obvious, it is complicated by the vast number of local service providers that are only concerned with last mile connectivity.³

In addition to Internet search, we appeal to the large number of existing Internet systems and publicly available data they provide. This includes PeeringDB [9], Network Time Protocol (NTP) servers, Domain Name System servers (DNS), listings of Internet Exchange Points (IXPs), Looking Glass servers, traceroute servers, Network Access Points, *etc.* Beyond their intrinsic interest, it is important to recognize that NTP servers [6] often publish their Lat/Lon coordinates and are typically co-located with other networking/computing equipment. Similarly, DNS servers routinely publish their location via the LOC record [18]. In total, over 4,700 network resources of various types are annotated in the Internet Atlas database.

3.2 Transcription of Network Data

Once a target network has been discovered via search, we transcribe the information to Atlas’ GIS database. This is complicated by the varying data formats used by each provider. Network maps can range from images (such as the Sprint Network Map [14]), to interactive maps (such as, the Flash-based AT&T Map [2] and the Google Maps-based Level3 Map [5]).

Visualization-centric representations often reveal no information about link paths other than connectivity (*e.g.*, line-of-sight abstractions are common). For these we enter the network adjacency graph by hand into Atlas. However, some maps provide highly detailed geographic layouts of fiber conduit connectivity (*e.g.*, Level3 [5]). We transcribe these, maintaining geographic accuracy, into the Atlas using a process and scripts that (i) capture high resolution sub-images, (ii) patch sub-images into a composite image, (iii) extract a network link image using color masking techniques, (iv) project the link-only image into ArcGIS using geographic reference points (*e.g.*, cities), and (v) use link vectorization in ArcGIS to enable analysis (*e.g.*, distance estimation) of the links.

Node locations in primary source data are provided in four forms: Lat/Lon, street address, city or state. If none of these location types is provided, then the node is not entered

¹Such information is often available from ISPs since it aids in their sales and marketing efforts.

²The current search term library is entirely in English. Moving beyond English is an objective in future work.

³Mapping last mile connectivity is a future goal for Internet Atlas.

into the repository. All node locations are geo-coded into the Atlas repository as a Lat/Lon, while maintaining the source information as meta data. If a Lat/Lon for a network resource is provided, that is transcribed directly into the repository. If a street address for a resource is provided, that address is translated into a Lat/Lon using ArcGIS’ inherent capabilities. If only a city/state location is provided, then that is translated into the Lat/Lon of the city/state center if no other more specific addresses for network infrastructure are available in that city/state. Otherwise, the Lat/Lon of the location in that city/state that has the most references from other networks is used. While clearly this could be inaccurate, we believe it is likely to be more accurate than simply leaving the location in the city/state center.

Provider maps often contain additional information about network node resources. This information can range from location (potentially down to Lat/Lon coordinates), to IP addresses, to resource or service types. Our ability to extract network node information from the discovered resources is dependent on an assembly of scripts that include Flash-based extraction and parsing tools [3], optical character recognition parsing tools [7], PDF-based parsing tools [8], in addition to standard text manipulation tools. This library of parsing scripts can extract information and enter it into database automatically. For instances where none of the tools or scripts are successful on the provider data, we manually parse and enter the data.

As an example, consider the map of the Layer42 [4] network, which is shown in Figure 2 (upper left). To extract the node, link and text information from the image, we convert it to CMYK color model and consider the *yellow* (third) and *magenta* (second) channels to identify nodes and edges respectively. If we then consider nodes and edges as connected components, we can construct a graph simply by identifying edges that touch a given node. We can then convert the input image to grayscale to find the text embedded in the image.

3.3 Verification and Updating of Network Data

Despite our efforts to automate the data transcription process, we still have to enter data manually from time to time. Thus, we must account for human error in this process. We employ several completeness and consistency checks to verify that that manually entered data accurately reflects the primary source data. These checks include having someone other than the person who entered the data manually compare it to the source data.

It is also important to recognize that network footprints will change periodically *e.g.*, a PoP will move from one hosting facility to another. Our goal is that the network maps in Atlas reflect current versions of primary source data. To that end, we periodically (quarterly) refer to previously identified primary sources and compare the current online information with the current representation in Atlas. Simple hashes of images enable potential changes to be identified. For network maps that have been automatically transcribed, we can use their vectorized images in Atlas as the basis for automated comparison.

Let the graph generated from the data in the Internet Atlas be $G_{atlas} : \{nodes_{atlas}, edges_{atlas}\}$. Let $G_{source} : \{nodes_{source}, edges_{source}\}$ be the new graph extracted from the primary source. Given the two graphs,

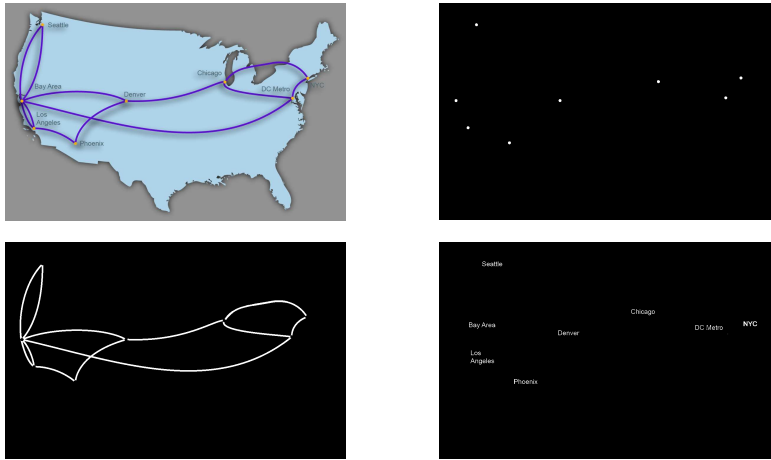


Figure 2: Original map of Layer42’s network [4] (upper left). Nodes (upper right), edges (lower left) and text (lower right) extracted by the Atlas automated parsing framework.

verification is checking if G_{source} and G_{atlas} are isomorphic. To facilitate this analysis, we use the proximity analysis capability available in ArcGIS. While this method is not infallible, it is useful for identifying changes.

Finally, it is important to distinguish between *verification* and *validation*. The former is meant to ensure the accuracy of the transcription process from source materials and that Atlas reflects the latest maps available from a primary source. We have taken significant steps to ensure the data in Atlas is verified. The latter is meant to ensure that the data reflects physical reality. It is entirely beyond the scope of our work to actually visit all locations, and we believe that this is an unreasonable standard. It is also clear that the current published maps may not reflect the most recent changes in a network. However, since we are using source information provided by ISPs (typically providing street or at least city addresses), we argue that there is already a high level of confidence in the data. Further, by virtue of the fact that *many* locations for PoPs appear in *multiple* networks, this is an further and important measure of self-consistency that increases confidence in the repository. We also avail ourselves of other data sources such as the CAIDA [17] and PeeringDB [9] repositories as means for additional consistency checks.

3.4 Precision of Network Data

The *precision* of the data in the Atlas repository is defined by the specificity of the locations in the primary source data. As noted above, nodes are entered into the repository based on the availability of at least one of four location types – Lat/Lon is the most precise and state name is the least. We use a separate column in the Atlas database to capture the precision of the data source. We follow a simple heuristic to assign values to each node. If the source data for a node has a Lat/Lon or street level address, then we assign a Source Score of 1.0. If the source data has only a city name, then we assign a Source Score of 0.75. If the source data has only a state name, then we assign a Source Score of 0.5. Table 1 depicts the precision of location information of all the nodes in our repository.

We use a similar designation for the precision of paths. While we cannot verify that maps that provide highly de-

Node Type	Source Score		
	0.5	0.75	1.0
Tier-1 PoPs	0	0	921
Other PoPs	0	8103	653
Data Centers	0	1886	273
DNS Root Servers	0	293	0
IXPs	0	0	358
NTP Servers	0	0	744
RIPE Servers	0	975	0
Traceroute Servers	0	221	0

Table 1: Precision of all the nodes in the Internet Atlas repository. A score of 1.0 indicates Lat/Lon or street-level precision, 0.75 indicates city-level precision, and 0.5 indicates state-level precision.

tailed geographic layouts of fiber conduit connectivity are accurate, we posit that such detail would not be provided if it were not accurate. Furthermore, visual inspection of many of these maps indicates that the paths typically follow major road/rail infrastructure, which is known to be common practice. This further enhances our confidence in the accuracy of the data.

3.5 Completeness of Network Data

While it is likely to be impossible to identify and include the locations of *all* buildings that house Internet infrastructure and the links that connect them in the Atlas repository, it is useful to know the relative contribution of adding new networks to the repository.

Figure 3 shows the growth of new nodes in the repository as new networks are added (using a greedy approach). Node overlap is defined by instances of identical Lat/Lon based on our geo-coding method describe above. The figure shows a gradual decay in slope indicating a decline in discovery of new nodes (link discovery shows a similar profile - omitted for brevity). This can be explained by the fact that much of the infrastructure for the larger networks is already included in Atlas while infrastructure for smaller networks is being added on an on-going basis.

3.6 Real-time Data Feeds

A key feature of Internet Atlas is the ability to include and visualize real-time data feeds in the portal. The current set of real-time data feeds include Twitter, BGPmon [27], and weather and disaster reports from NOAA and FEMA. Our intention in including this selection of data feeds is to demonstrate the flexibility and extensibility of our platform and to enable Internet Atlas to be used, for example, to analyze the risks of Internet infrastructure to natural disasters.

We use ArcGIS tracking server [1] as a tracking engine for the real-time data. The key capability of the tracking engine is to integrate real-time data feeds with the other geographic data in the repository. With the tracking server, one can receive data in any format and distribute it to clients, perform filtering and generate alerts based on attributes of data or spatial positions, and log the data for later use.

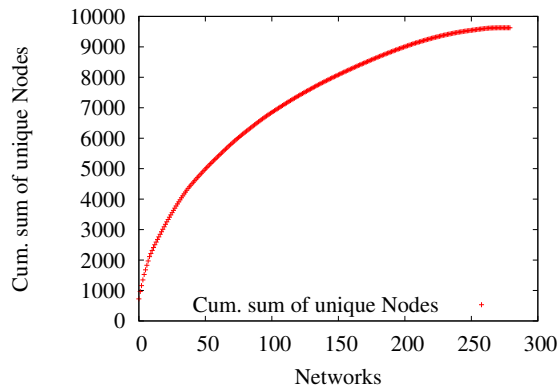


Figure 3: Number of unique nodes discovered as new networks are added to the Atlas repository.

Our primary task in extending the repository to include real-time data was to develop scripts to connect the tracking server to the various remote APIs. This is typically straightforward, but requires special capabilities for each data feed. For example, our interface to Twitter captures all tweets that include some mention of a network-related event. To that end, we have implemented a targeted dictionary of terms and phrases that we look before we archive a tweet (*e.g.*, hurricane, disaster, network failure, poor connectivity, topology change). We rely on Twitter’s reported coordinates for geo-coding understanding that these may not be accurate. Our approach is similar for the other data feeds. New data feeds will be added on an on-going basis.

3.7 Static Data

One of the important benefits of developing Atlas on top of ArcGIS is that we can immediately take advantage of a wide variety of geo-coded data sets that are available for that system. To demonstrate this capability, we currently include road and rail infrastructure in the US along with population data from the US census. This data can be used, for example, to assess the density of Internet infrastructure in different metropolitan areas or rights-of-way for future fiber conduits.

We also include daily downloads of Internet attack data from DSHIELD.org. DSHIELD data includes the source IP addresses of attacking nodes from over 1700 networks world-wide [28]. We currently use MaxMind to geo-code the locations of attacking nodes. While the accuracy of IP geo-coding is a subject of on-going work, our intention is

simply to demonstrate the capability of Atlas in the area of security.

4. INTERNET ATLAS PORTAL IMPLEMENTATION

In this section, we describe the implementation of Internet Atlas, including the web portal, the ArcGIS-based visualization and analysis engine, and the network information database.

4.1 Internet Atlas Web Portal

Our overall goal in developing a web portal for Atlas was to provide a visualization and analysis environment that would make the underlying repository useful for both research and operations. Specific technical goals included making the portal highly responsive, scalable, extensible and secure.

To accomplish these goals, we implemented the portal in Java and JSP using the Spring Framework [13], which enables access from any web browser and enables declarative, annotation-driven support for transactions and caching. Similarly, Spring Security provides a highly customizable authentication and user access-control framework. We also use Adobe’s Flex SDK [16] to build dynamic applications on top of the ArcGIS server.

The primary challenge that we faced in developing the web portal was to balance the ease-of-use and flexibility, with security for the underlying data. We addressed that challenge by leveraging the powerful collection of performance and authentication APIs provided by Spring Framework. Every critical aspect of the portal has been modeled using interface-driven design principles to ensure flexibility and security.

Internet Atlas runs on an Apache Tomcat 6.0 web server installed on a Intel-based Red Hat Enterprise Linux machine.

4.2 Visualization via ArcGIS

We use ArcGIS Version 10.1 [19] as visualization engine for the data in our repository. ArcGIS enables base maps of the earth or other infrastructures (*e.g.*, roads or rails) to be displayed in layers below individual network maps or aggregates of network maps. The system also provides basic spatial navigation, which is critical for examining maps at multiple scales. In addition, the use of ArcGIS allows for fine-grained control over the data access (*e.g.*, in contrast to Google Maps) and the ability to use openly available data processing and spatial analysis tools that have been written to the ArcGIS standard.

ArcGIS is accessed by the web portal through Adobe’s Flex. The challenges in developing this capability were primarily in creating and deploying a custom GIS web-mapping application that supports data display, interactive querying, and geocoding. We addressed these challenges by leveraging the extensible widget programming model supported by Adobe’s Flex.

4.3 Internet Atlas Database Structure

The ArcGIS system references our database repository, which contains the physical network data, real-time feeds and static data. The repository also contains meta-data, including source provenance (*e.g.*, where and when data was

acquired), IP address ranges associated with ISPs, the perceived confidence in the observed data, and other relevant information on the service provider's network. We also archive snapshots of all network maps and data.

The backend data repository is based on MySQL. The repository contains 16 tables that captures the various source information described above. The current size of the repository (excluding the real-time data) is 92 MB.

5. SUMMARY AND CONCLUSIONS

In this paper, we describe the Internet Atlas project. The goal of our work is a visualization and analysis environment that is based on a geographically accurate map of the physical Internet. We assemble this physical representation of the Internet using search to identify maps and other repositories of the locations of buildings that house networking equipment and the conduits that connect them. We have developed a substantial collection of scripted tools that automate many aspects of identifying, verifying, collecting and transcribing maps of physical Internet infrastructure into the Atlas database repository.

The Atlas data repository is available through an openly available web portal. This system is based on the widely-used ArcGIS geographic information system, which includes a spatial database that enables flexible aggregation and visualization of diverse, geo-coded data sets. ArcGIS also includes a large set of built-in tools that enable a broad set of spatial and statistical analyses.

The current Internet Atlas repository includes maps and associated meta-data from over 270 networks world wide (including all tier-1 providers). This data comprises over 9.5K PoPs and over 13.5K links. The repository also includes locations for other Internet infrastructure such as NTP, DNS and looking glass servers. To further increase the utility of Atlas, we extend the repository with relevant, related real-time feeds (*e.g.*, BGP updates, Twitter feeds, and weather data) and static data (*e.g.*, DSHIELD logs, road/rail infrastructure).

In future work, we will continue to expand the Internet Atlas by adding additional maps as they are discovered in on-going search campaigns. We will also begin further expansion and diversification of the repository *e.g.*, by adding real time measurement capability.

Acknowledgements

The authors would like to thank Mike Blodgett and Math Heinzl for their contributions to this project. This work was supported in part by NSF grants CNS-0831427, CNS-0905186, ARL/ARO grant W911NF1110227 and the DHS PREDICT Project. Any opinions, findings, conclusions or other recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF, ARO or DHS.

6. REFERENCES

- [1] ArcGIS Tracking Server. <http://www.esri.com/software/arcgis/tracking-server>.
- [2] AT&T Network Map. <http://www.corp.att.com/globalnetworking/>.
- [3] FlashGot. <http://www.flashgot.net/>.
- [4] Layer42 Network Map. <http://www.layer42.net>.
- [5] Level3 Network Map. <http://maps.level3.com/>.
- [6] Network Time Protocol Project Website. <http://www.ntp.org/>.
- [7] OnlineOCR. <http://www.onlineocr.net/>.
- [8] PDF2XL. <http://www.cogniview.com>.
- [9] PeeringDB, Exchange Point List. <https://www.peeringdb.com/>.
- [10] Route Views Project. <http://www.routeviews.org/>.
- [11] SidePad. <http://www.sidepad.gov/>.
- [12] Soovle. <http://www.soovle.gov/>.
- [13] Spring Framework. <http://www.springsource.org>.
- [14] Sprint Network Map. https://www.sprint.net/network_maps.php.
- [15] The Internet Atlas. <http://atlas.wail.wisc.edu/>.
- [16] Adobe. The Flex SDK. <http://www.adobe.com/devnet/flex.html>.
- [17] CAIDA. The Skitter Project. <http://www.caida.org/tools/measurement/skitter/>, 2007.
- [18] C. Davis, P. Vixie, T. Goodwin, and I. Dickinson. A Means for Expressing Location Information in the Domain Name System. <http://tools.ietf.org/rfc/rfc1876.txt>.
- [19] ESRI. ArcGIS Geographic Information Systems. 2012.
- [20] S. Gorman. *Networks, Security And Complexity: The Role of Public Policy in Critical Infrastructure Protection*. Edward Elgar, 2005.
- [21] S. Knight, H. Nguyen, N. Falkner, R. Bowden, and M. Roughan. The Internet Topology Zoo. <http://www.topology-zoo.org>.
- [22] H. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani. iPlane: An Information Plane for Distributed Services. In *Proceedings of the 7th USENIX OSDI '06*, Seattle, WA, November 2006.
- [23] Z. Mao, J. Rexford, J. Wang, and R. Katz. Towards an Accurate AS-Level Traceroute Tool. In *Proceedings of ACM SIGCOMM 2003*, Karlsruhe, Germany, August 2003.
- [24] V. Paxson, A. Adams, and M. Mathis. Experiences with NIMI. In *Symposium on Applications and the Internet Workshops*, Los Alamitos, CA, 2002.
- [25] Y. Shavitt and E. Shir. DIMES: Let the Internet Measure Itself. *ACM SIGCOMM Computer Communications Review*, 35(5), October 2005.
- [26] N. Spring, R. Mahajan, D. Wetherall, and T. Anderson. Measuring ISP topologies with Rocketfuel. *IEEE/ACM Transactions on Networking*, 12(1), 2004.
- [27] H. Yan, R. Oliveira, K. Burnett, D. Matthews, L. Zhang, and D. Massey. BGPmon: A Real-Time, Scalable, Extensible Monitoring System. In *Proceedings of the CATCH '09*, Washington, DC, March 2009.
- [28] V. Yegneswaran, P. Barford, and J. Ullrich. Internet Intrusions: Global Characteristics and Prevalence. In *Proceedings of ACM SIGMETRICS*, San Diego, CA, June 2003.
- [29] B. Zhang, R. Liu, D. Massey, and L. Zhang. Collecting the Internet AS-Level Topology. *SIGCOMM Computer Communication Review*, 35(1):53–61, January 2005.