NAFD

1: Introduction

Network/Internet-scale Disruptive Events (NIDEs) can disrupt the Internet connectivity of thousands of users and affect Internet resilience at large. CAIDA’s IODA system [12] detects macroscopic Internet-edge outage events, a class of NIDEs that we define in the project deliverable NIDE Identification Document (NID). Broadly, a macroscopic Internet-edge outage event is a connectivity disruption happening at the edge of the Internet topology affecting a large geographic area or an Autonomous System. These events can be caused by several factors, including natural disasters, severe weather, misconfiguration, and DoS attacks.

In Section 2 of this document, we describe the current IODA methodological approach to detect macroscopic Internet-edge outage events using three distinct types of data sources: Internet Background Radiation (IBR), BGP, and active probing. We discuss IODA’s rationale and methodology for detecting outage events for each data source and highlight challenges in performing this detection accurately and efficiently.

In Section 3, we describe several methodological enhancements of the IODA system. These enhancements will improve IODA’s accuracy, reduce the latency of outage detection, and increase IODA’s coverage.

2: Measurement and detection methodology

2.1. Overview

To detect macroscopic Internet-edge outage events, CAIDA’s IODA system employs three data sources, each of which offers visibility into different aspects of global Internet connectivity. Fusing event signals extracted from these data sources increases IODA’s overall coverage. Moreover, by analyzing how an event manifested itself across various data sources, we learn hints about its potential underlying cause(s).

IODA considers outages affecting various address aggregates, thus providing additional context to event characterization. An address aggregate is a set of addresses related to each other, for example, belonging to the same Autonomous System (AS) or geographic region. Our insight is that events with a significant impact on network connectivity will likely affect hosts belonging to the same address aggregate. Thus, for each data source, the IODA system currently looks for
outages affecting address aggregates of three types: by country, by region (such as U.S. state or Canadian province), and by AS.

For all three data sources, the current macroscopic Internet-edge outage detection scheme is based on the same premise: that a drop in the time-series signal for a given data source for a specific address-aggregate is indicative of a possible outage. To detect such a drop, we compare the current value for each data source/aggregation (e.g., the number of /24 networks visible on BGP and geolocated to Italy) to a historical value computed as the median across a sliding window of recent values. The length of the window varies between data sources and is listed below for each data source.

### 2.2. Per-source methodologies

#### 2.2.1. Internet Background Radiation (IBR)

IBR is one-way unsolicited traffic generated by millions of Internet hosts worldwide. This unsolicited traffic is caused by scanning (e.g., searching for hosts running a vulnerable service), misconfigurations (e.g., a typo in the IP address for a mail server), backscatter (responses to packets with forged source IP addresses, including spoofed DoS attack), bugs, etc. A network telescope is a collection of routed but unused IP addresses used to capture unsolicited traffic. The IODA system’s source of IBR data is the UCSD Network Telescope, which observes traffic sent to more than 90% of IP addresses in a contiguous /8 block.

IODA is the only outage inference system using IBR, thanks to a methodology that we demonstrated is capable of detecting outages caused by state censorship, natural disasters, and border router misconfiguration. Our intuition is that the wide prevalence of IBR traffic results in continuous traffic reaching our network telescope from almost any aggregate of addresses (such as addresses from a geographic region or AS). We therefore use the IBR traffic from an address aggregate as a liveness signal indicating that addresses in the aggregate are able to send traffic to the Internet. When traffic from an aggregate ceases to arrive at our telescope, we infer that that aggregate of IP addresses is experiencing an outage.

**Challenges**

- **IBR traffic can include packets with spoofed source addresses.** If not filtered out, these packets have the potential to pollute our inferences. However, since network telescopes normally only see incoming traffic and do not respond, confirming that the source address in a packet corresponds to the address of the sender is a technical challenge.

- **The UCSD network telescope observes insufficient IBR data from some address aggregates.** For address aggregates with few overall IP addresses (such as small countries or geographic provinces), there may be not be enough traffic to extract a signal useful for outage detection.
- The IBR data is unpredictable and erratic in nature and the data evolves over time [1]. Since it is a mix of a broad range of phenomena leading to unsolicited traffic, with new phenomena continuously emerging, IBR can significantly change its characteristics over time (e.g., new bursty components can appear temporarily or for a prolonged period of time), not just in terms of packets and bytes, but also in the number of sources sending the traffic.

- Accurate detection of outages with the IBR data is challenging. Identifying outage detection thresholds that are sensitive enough to detect real outages but are not so sensitive as to falsely detect outages that did not happen, is a non-trivial task for all data sources. It is particularly challenging for the IBR data-source since some address aggregates may have little traffic to begin with, and this traffic can fluctuate and may include spoofed source addresses. Thus, covering more address aggregates could come at the price of detecting more false positive and negative events for those aggregates.

- High volume of data at the UCSD network telescope impedes identification and analysis of outages in near real-time. With over 300 Mbps of traffic constantly arriving at the network telescope (and frequent periods of rates up to and exceeding 1 Gbps), we need sophisticated, highly-optimized filtering and analysis algorithms.

Methodology
We collect IBR traffic through the UCSD Network Telescope, an almost entirely unutilized /8 IPv4 address block, that observes approximately 1/256th of all the IBR generated in the Internet. As of September 2018, the telescope captures more than 1.5 TB of compressed traffic per day. We process this traffic in 1-hour batches using our Corsaro open-source software platform. To address spoofed traffic and bursty traffic components in the IBR data, we pass the data through several filters. We build signatures for our filters by identifying suspicious traffic components, manually isolating and analyzing them, and then defining a filter to remove them. Next, we extract a “liveness signal” for each address aggregate, based on the number of distinct source IP addresses observed from that aggregate. We use this metric (e.g., instead of packet count) because it provides us with a proxy for a count of active devices in an address aggregate. We examine the timeseries of the liveness signal to detect macroscopic Internet-edge outages. When the number of distinct source IP addresses for an aggregate drops below 25% of the median value calculated over the last seven days, a warning alert is generated. When the drop is below 10%, a critical alert is generated.

Pros:
- The IBR data source offers visibility into many diverse address aggregates since the amount of IBR that reaches network telescopes is considerable, incessant, and originates from a variety of networks and applications.
- Since IBR traffic is spontaneously sourced by the same addresses that we seek to monitor, we are not thwarted by filtering (whereas packet probes used in active measurements can be -- and often are -- filtered).
- We create no additional network overhead since we do not introduce additional probes into the network.

Cons:
- The opportunistic nature of the IBR traffic measurement and analysis prevents us from analyzing arbitrary address aggregates; instead, we are limited to the address aggregates generating a sufficient amount of IBR traffic.

- Since IBR traffic is subject to large fluctuations, there is potential for false positive and false negative detections.

Key areas for improvement:
- *Improve the accuracy of the outage detection methodology.* There is a tradeoff between the sensitivity of the outage detection approach and its accuracy. Our current thresholds are statically determined and err towards false negatives, ideally so that we only detect outages that we are confident in. However, even with these conservative thresholds, we still observe many false positives due to the highly variable nature of the IBR traffic. More advanced models and predictive algorithms would allow us to significantly improve detection accuracy.

- *Improve the latency with which we report detected outages.* At present, detection is performed by processing 1-hour batches of IBR traffic. As traffic rates at the telescope have increased over the 6 years since we initially developed our analysis software, we are now barely able to process data in real-time (i.e., it often takes us longer than 1 hour to process a 1 hour traffic batch), and so any system failures or delays quickly add up—we have had several occasions where detection was delayed by as much as two days.

2.2.2. BGP routing information

As the de-facto inter-domain routing protocol for the Internet, the Border Gateway Protocol (BGP) enables ASes to exchange reachability information with each other. Each AS announces to the others, by means of BGP update messages, the routes to its local prefixes and the preferred routes learned from its neighbors. These messages provide information about how a destination can be reached.

The IODA system monitors BGP messages sent by hundreds of Internet routers and uses them to infer connectivity problems. Since BGP messages contain information on how to reach destinations, they can also be leveraged to reason about when destinations are unreachable. We use BGP messages to understand whether a set of prefixes (e.g., those that share the same geographical region, or the same origin AS) are globally reachable or not.

Challenges:
- **Multiple vantage points (VPs) are required to assess the reachability of a BGP prefix.** Information from a single VP is not sufficient to verify a BGP prefix’s unreachability; in fact, a prefix may be not reachable from a given VP because of a local routing failure. On the other hand, if several VPs, topologically and geographically dispersed, simultaneously lose visibility of a prefix, then the prefix itself is likely undergoing an outage.

- **The states of the routing tables from multiple vantage points need to be reconstructed at regular intervals.** Since detecting outages requires comparing the prefix reachability information as observed from multiple VPs, each inferred routing table needs to be continually updated. This requires the maintenance of a global (i.e., for every VP) view of BGP reachability information updated with fine time granularity (e.g., few minutes).

- **BGP routing data requires additional filtering and processing before it can be used for outage detection.** In the absence of such filtering, potential anomalies in the BGP data source—such as route leaks and level shifts (which, for example, can occur when a prefix is announced)—can result in false outage inferences.

- **BGP prefixes can vary in size.** If a /24 BGP prefix has an outage, 256 addresses are affected by the outage. On the other hand, if a /8 BGP prefix has an outage, 16.8M addresses may be affected. Thus, outage detection with the BGP data source should not simply consider how many prefixes are visible per address aggregate but also how many addresses these prefixes contain.

- **A BGP prefix can sometimes geolocate to different geographic regions.** The naive approach to prefix geo-location—simply mapping each IP address to its corresponding geo-location—can be insufficient: a larger prefix may fully contain another announced prefix that maps to a different geographical location but the larger prefix might not be related to the second geographical location at all.

**Methodology:**
To obtain multiple vantage points, we leverage the collection infrastructure operated by the RouteViews and RIPE RIS projects using CAIDA’s BGPStream framework [5] and continuously process data from more than 300 operational BGP routers. The Routeviews and RIPE RIS projects offer broad coverage as they include BGP route collectors in many ASes and regions. We infer the state of the routing tables exported by hundreds of operational routers by processing BGP updates and RIB dumps and we extract information about which network blocks (BGP prefixes) appear reachable on the Internet control plane from most of these vantage points.
Different from other organizations occasionally reporting BGP-visible connectivity disruption (e.g., Renesys/Dyn), our approach counts visible /24 blocks (i.e., the number of /24 blocks that are covered by visible prefixes) instead of prefixes, more meaningfully quantifying which fraction of the address space normally announced by an AS or from a region is reachable at a certain point in time. We examine the timeseries of the visible /24 blocks in an address aggregate to
detect macroscopic Internet-edge outages. When the number of the visible /24 blocks for an aggregate drops to below 99% of the median value over the last 24 hours, a warning alert is generated. When the drop is below 50%, a critical alert is generated.

**Pros:**
- Outages detected by BGP routing are likely to be highly accurate. When a control-plane path to a destination prefix does not exist, addresses in the prefix are unlikely to be able to communicate over the Internet.

- The BGP data source introduces little additional measurement traffic into the network.

**Cons:**
- Since BGP messages indicate connectivity (or the lack thereof) in the control-plane, the BGP routing dataset allows us to detect only the subset of outages that affect the control-plane.

**Key areas for improvement:**
- Detect outages accurately even when prefixes geolocate to multiple geographic regions.

### 2.2.3. Active probing

Active probes, such as pings and traceroutes, are widely used network diagnostic tools. Probes can be sent using different protocols, including ICMP, UDP, and TCP, to any host on the Internet. Recent work has shown that more than half of the active IPv4 addresses in the Internet respond to ICMP probes [11]. Thus, techniques using active probes can measure broad swaths of the Internet's address space at fine granularities.

Active probes can be used to determine the reachability of end-hosts. A response from a probed address generally implies a working Internet connection. Non-responses could be indicative of connectivity problems. Thus, several techniques have employed active probes to infer the connectivity of Internet-edge addresses [9, 10].

**Challenges:**
- Several confounding factors influence interpreting of active probe responses (or the lack thereof). Lack of response to active probes from addresses is assumed to be a sign that the edge Internet hosts to whom those addresses are assigned have an Internet connectivity outage. However, this assumption may be untrue if probe responses cease to arrive as a result of end-user action (such as the user powering off their home router equipment). This assumption may also be untrue if ISPs perform prefix migration, where they move edge Internet hosts en-masse to a different part of the address space [4].

- Rate-limiting of active probes by some networks presents a tradeoff between probe traffic volume and the precision and accuracy with which edge Internet outages can be detected. If probes are sent to destination networks too quickly, they may be rate-limited and responses
may be harder to interpret [4]. However, if probes are sent too infrequently, outages that affected only a few addresses or lasted for a relatively short time may not be detected.

- **Outages detected using the active probing source could be a background noise.** Active probing enables the detection of outages at finer (address space) granularities compared to the IBR and BGP data sources, including at the granularity of /24 address blocks [9] or even individual addresses [10]. However, not every instance of an individual address outage or even an individual /24 outage constitutes a macroscopic Internet-edge outage. A variety of factors, including user behavior (such as a residential user switching off their home Internet equipment), dynamic addressing renumbering, or even scheduled maintenance [4], can result in an outage of a /24 address block. A macroscopic Internet-edge outage, however, is a more significant event, involving the failure of many related addresses (or /24 blocks). Thus, identifying macroscopic Internet-edge outage events in the presence of background noise is a challenge.

**Methodology:**
We periodically probe approximately 3.5 M /24 network blocks worldwide and adaptively send more probes upon lack of response using the Trinocular methodology developed by ISI/USC [9]. Our active probing system models the responsiveness of blocks and finds subsets of addresses within each block that are likely to respond to pings using historical data from the ISI census [2]. The system chooses a few of these addresses from each block at random for each round of probing. We probe in 10-minute rounds. We employ Bayesian inference to reason about responses from blocks. When a block's responsiveness is lower than expected, our active probing system probes the block at a faster rate and eventually detects an outage when the follow-up probes also indicate the block's lack of Internet connectivity.

We examine the timeseries of the /24 address blocks that are “up” in an address aggregate to detect macroscopic Internet-edge outages (an address block that is responsive to probes is “up”). When the number of “up” /24 blocks for an aggregate drops to below 80% of the median value over the last seven days, a warning alert is generated. When the drop is below 50%, a critical alert is generated. By probing only a few addresses in each /24 in a 10-minute round, we keep the volume of probing traffic low and avoid rate-limiting. Since we detect outages affecting most addresses in a /24 address block, detected events are unlikely to be caused by individual users’ actions. Further, since we only detect a macroscopic Internet-edge outage when there is a drop in the “up” /24s for an entire aggregate, we mitigate the prefix migration problem [4].

**Pros:**
- Active probing can find data-plane outages that may be invisible to the control-plane.

- Active probing complements the data-plane view offered by the IBR data. Some address aggregates may not generate sufficient IBR traffic to enable outage detection; however, addresses may respond to active probes.

- Active probing allows us to control which addresses to probe and the rate at which probes are sent to addresses.
**Cons:**
- Some destination networks filter active probing traffic. For such networks, it is impossible to detect disruptions using active probing systems.
- Active probing introduces additional traffic into the Internet. Though the volume of probe traffic sent by our active probing system towards individual networks is small, some networks might perceive probe traffic as malicious or a burden.

**Key areas for improvement:**
- Identifying which outages of /24 address blocks detected by IODA constitute a macroscopic Internet-edge outage. Our preliminary investigations suggest the presence of background noise; some /24 address blocks appear to have unusually many outages.
- We can improve accuracy by evaluating the outages detected by the active probing data source against publicly available outage data provided by other research efforts.

**3: Methodological Improvements to IODA**

In this section, we describe our approaches for improving macroscopic Internet-edge outage detection with the IODA data sources. These enhancements constitute Task 1.2 from the Statement of Work: “Develop Internet measurement, data collection, sanitization, aggregation and analysis methodologies to detect the events defined in Task 1 in near-real-time”.

**3.1. Improving the accuracy of outages inferred using the IBR data source**

When using the IBR data source, the current IODA system is designed to detect only large macroscopic Internet-edge outages, reducing incorrect inferences due to the fluctuating bursty nature of the IBR traffic. Recall that the IBR time series signal that we use for outage detection for a given address aggregate is the number of distinct source IP addresses in this aggregate originating traffic towards our darknet. Compared to the time series signals from BGP and active probing, the IBR signal exhibits far higher fluctuation, especially for smaller aggregates such as Autonomous Systems (ASes) and provinces within countries. To reduce false positives, our thresholds to detect an anomalous drop in the time series signal of IBR data for an aggregate are rather conservative. For example, we currently raise an outage alert in an address aggregate only when the signal drops below 25% of the median value observed in the last 7 days. Consequently, the current IODA system will only detect very large macroscopic Internet-edge outage events using the IBR data source.
In collaboration with researchers from Internet Initiative Japan (IIJ) and the University of Strasbourg, we are investigating how to improve macroscopic Internet-edge outage detection with IBR data. Preliminary investigations using the Seasonal Autoregressive Integrated Moving Average (S-ARIMA) time-series anomaly detection technique, suggest that we can detect more outages while remaining highly accurate. We chose the S-ARIMA model since it can learn and predict time-series signals containing periodic elements; our preliminary results show that the IBR data source's time-series signal has a weekly pattern. A S-ARIMA model can forecast the behavior of the time series for each address aggregate. When an observed value is much lower than the predicted value, we detect an outage. We have found that this prediction model appears to be robust to the seasonality and noise observed in the data.

The use of S-ARIMA for outage detection with the IBR data is currently in the proof-of-concept stage. We are investigating the best combination of parameters for the S-ARIMA model such that the accuracy of detected outages remains high. After tuning the parameters and evaluating accuracy, we will integrate the S-ARIMA outage detection technique into the IODA system for the IBR data.

3.2. Inferring outages from the IBR data source in near-realtime

Currently IODA performs outage detection on IBR data by processing traffic in 1-hour batches, giving us a theoretical minimum detection latency of 1 hour. However, as traffic rates at the telescope have increased dramatically in the 6 years since we initially developed our analysis software, we are no longer able to process data in real-time (i.e., it often takes us longer than 1 hour to process a 1 hour batch of traffic), and as such, detection latency is usually around 2 hours, with frequent delays of many hours or even days, if we have any system or processing failures.

To address this problem, we are developing state-of-the-art real-time data collection, distribution and analysis systems for the IBR data source that are capable of keeping up with current and projected traffic rates. The efficient collection and processing of IBR traffic at the UCSD Network Telescope is relevant to other research projects and infrastructure operated by UC San Diego and is co-funded by NSF grant CNS-1730661 (STARDUST project). As part of the IODA-NP project, we will build efficient, high-speed traffic analysis software that sanitizes, augments with meta-data tags, and analyzes IBR traffic data in order to extract the high-level signals used by IODA's outage detection modules. This platform will directly process traffic as it arrives at the telescope, thus reducing the detection latency to approximately 2 minutes.

To achieve this level of efficiency, we are developing a pipeline of high-performance real-time traffic analysis modules. Due to the high constant packet rates and frequent short-term spikes in the traffic collected by the UCSD Network Telescope, avoiding data loss while processing real-time data requires highly-optimized, distributed software architectures. With this in mind, we will design and implement modules to:
1. Identify and tag packets based on previously developed heuristics for detecting erratic traffic components and IP spoofing.
2. Query IP meta-data databases and map source IP addresses to origin ASN and geographic area (e.g., country, region, county).
3. Extract high-level time series signals for different traffic aggregations and store them in IODA's time series databases.

3.3. Improving the geolocation of BGP prefixes

The current IODA system can detect outages incorrectly when a BGP prefix geolocates to multiple regions. Since BGP prefixes differ greatly in size—a /8 prefix contains 4M addresses whereas a /24 one contains only 256 addresses—IODA uses a normalized view of BGP prefixes per geographic region by tracking the number of /24 address blocks per region. However, consider when IODA observes a macroscopic Internet-edge outage for a BGP prefix, a.b.0.0/16. To determine which countries lost connectivity for those addresses, IODA will geo-locate all of the prefix’s $2^{16}$ addresses. If all of the addresses are in the same country, then IODA will correctly infer that 256 /24 address blocks in that country had an outage. However, if a.b.c.0/24 is in South Africa and all remaining addresses are in Zimbabwe, then IODA will incorrectly infer that 256 /24s for both these countries had an outage. In addition, in the case a.b.c.0/24 is also announced, it is unclear if the control-plane visibility of the prefix a.b.0.0/16 can be related at all to the reachability of the addresses within the /24 block in South Africa. This is an inherent ambiguity that exists in BGP prefix visibility data when attempting geolocation inference.

We will address this challenge along two mutually complementary directions:

1. We will study the extent of the problem (e.g., how frequently overlapping BGP prefixes geolocate to different geographic regions, such as countries or cities). We will next investigate new methods to associate IP geolocation data with larger prefix blocks covered by overlapping sub-prefixes.
2. We will design, implement, and test new algorithms and data structures for IODA that are capable of handling instances where a BGP prefix geolocates to multiple regions. E.g., since in IODA we count the visibility of /24 blocks (based on the visible BGP prefixes that cover them), we will introduce a prefix geolocation mechanism that operates at /24 granularity: e.g., in the first example above, only one /24 block from South Africa and 255 /24 blocks from Zimbabwe will be counted as experiencing an outage.

3.4. Integrating the Thunderping active probing methodology into IODA

The Thunderping system detects failures of individual addresses during severe weather [10]. The system pings sampled addresses from multiple ISPs in geographic areas in the United
States. Originally designed to evaluate how weather affects Internet outages, the system uses Planetlab vantage points to ping 100 IPv4 addresses from multiple ISPs in each U.S. county with active weather alerts. Each address is pinged from multiple Planetlab vantage points (at least 3) every 11 minutes, and addresses in a county are pinged six hours before, during, and after a weather alert for that county. Analysis of these responses has revealed that severe weather is often correlated with increased probability of outages.

Thunderping’s measurements of outages affecting individual addresses are complementary to the outages measured by the other data sources in IODA. Its focused probing of sampled addresses in geographical areas subject to severe weather can reveal outages that affect smaller address aggregates, such as the those in a single U.S. county or zip-code. We will experiment with the Thunderping methodology and data in two ways:

1. Detect macroscopic Internet-edge outages using the Thunderping data source in spite of the presence of background noise:

   The IODA system detects macroscopic Internet-edge outages when there is a drop in the time series signal from its data sources—or in other words, when many addresses experience a simultaneous outage. However, when monitoring address aggregates consisting of many thousands of individual addresses—such as all of Thunderping’s sampled addresses in the U.S.—it is possible that some addresses experience a simultaneous outage by random chance. These outages may occur due to user behavior (such as a residential user switching off their home router), dynamic addressing renumbering, or even scheduled maintenance. We call outages occurring simultaneously by random chance background noise.

   We will develop an approach that can distinguish between background noise and macroscopic Internet-edge outages. Our intuition is that macroscopic Internet-edge outage events will result in simultaneous outages of many IP addresses such that these failures are unlikely to have occurred in a statistically independent manner. On the other hand, outages due to background noise will typically occur in a statistically independent manner. Our approach is to model individual address outages as independent events; when outages co-occur in greater numbers than the independent model can explain, the outages must be dependent. Binomial testing provides this ability to find events that are highly unlikely to have occurred independently. For example, when observing N addresses in an address aggregate (such as all pinged addresses in a certain geographic area, like San Diego), the Binomial distribution yields G, the minimum number of addresses in that aggregate that need to fail for the event to be considered an actual outage (many related addresses losing connectivity at the same time sharing the same cause) instead of background noise. Preliminary results obtained through the application of the Binomial testing approach to the Thunderping data offer promise; however, substantial work remains in parameterizing the Binomial test for various address aggregates. Depending upon our success with this approach and the Thunderping data source, we will also investigate it for outage detection with the other IODA data sources.
2. Compare and contrast IODA’s current /24 address block probing scheme against the Thunderping methodology:

IODA’s current active probing data source applies the Trinocular methodology [9], which uses probe responses to make inferences about an entire /24 address block. The Thunderping methodology [10], on the other hand, pings individual IP addresses and infers connectivity (or lack thereof) of individual addresses. By probing only a few addresses in the /24 in each round, the Trinocular methodology keeps the probing volume (towards each /24 address block) low. However, it will not identify an outage if even a single address in a block responds to probes. Trinocular could therefore miss outages that affect /24 blocks only partially, including macroscopic Internet-edge outages affecting multiple /24 blocks. To quantify the extent to which Trinocular misses outages, we will use the Thunderping methodology’s individual address outage data and determine how often Thunderping’s outages affected /24 blocks only partially. We will use these results to determine the accuracy and coverage of the Trinocular methodology and will investigate more widespread probing schemes based upon the results.

3.5. Detect macroscopic Internet-edge outages affecting finer address aggregates

At present, the IODA system detects outages affecting the following types of address aggregates: country, region (such as U.S. state or Canadian province), and AS. While these three address aggregates give IODA visibility into many types of outages, we lack the ability to detect and visualize outages affecting only a small geographic area. For example, a city-wide power outage could affect Internet connectivity of many users, but may not be large enough to noticeably affect the baseline signal of the region or of any individual AS.

To address this gap in IODA’s coverage, we are investigating the possibility of performing outage detection in smaller geopolitical address aggregates, such as U.S. counties and ZIP codes. But identifying sub-regional geopolitical areas for all countries in the world requires considerable manual effort. Thus, as a proof-of-concept, we plan to start with the U.S., since U.S. counties and ZIP codes are well-defined sub-regional geopolitical areas. To this end, we will first work to extend our IP geolocation libraries and databases to support county-level geo-location of US-based IP addresses. We will then extend the analysis components for each of our three data sources to support generating per-county signals using this new county-level geolocation capability. We will also enhance our detection module to monitor these new signals in order to detect outages affecting U.S. counties. Finally, we will modify the IODA web dashboard to support visualization and inspection of detected county-level outages.

3.6 Fusing outage inferences from the different data sources

Fusing inferences from the three IODA’s data sources can provide additional insight about detected outages. Currently, IODA detects macroscopic Internet-edge outages from each data
source independently. This design choice enables IODA to identify outages that are only visible to a subset of the data sources; for example, a power outage in a neighborhood may only be visible in the active probing dataset, since it does not affect BGP and the amount of IBR from the neighborhood is negligible. However, some outage events may be visible in more than one data source. For example, an outage caused by Internet censorship may be visible in all three data sources. Combining outage inferences from all of our data sources can improve our confidence that a detected anomaly is a macroscopic Internet-edge outage. Further, by fusing inferences, we may gain insight into the underlying cause(s) of the outage.

We will develop a methodology to fuse outage inferences into a single combined signal and triggering alerts with a higher confidence level when inferences match. Our approach for analyzing the time series signals from the data sources is to calculate a fusion score. IODA’s current per-data source detection yields two values when an alert is generated: a relative drop and duration. The relative drop indicates the ratio between the value of the signal during the outage and the baseline (i.e., non-outage) signal. For example, a signal that drops from a baseline of 100 to 75 during an outage would have a relative drop of 25%. The duration is simply how long the detected outage lasted (or how long since it began if the outage is ongoing). By multiplying these two values together we obtain an alert score. (Multiplying relative drop by duration allows both short-lived but significant, as well as long-lived but relatively minor outages to be captured.) We will extend this system to identify related per-data source events and multiply the corresponding alert scores together into a single fusion score. We will use multiplication (e.g., rather than addition) to combine alert scores so that we highlight events detected by multiple data sources. Since a single outage may manifest differently (e.g., with different latency) depending on the data source(s) that detect it, we will experiment with different methods and thresholds for grouping related events.

4: Evaluating IODA

We will validate the macroscopic Internet-edge outages detected by the IODA system by comparing IODA’s detected outage events against instances of well-known outage events from ground-truth sources. A variety of sources can potentially provide ground-truth. For example, news media sometimes report on widespread outages. Users on the Nanog mailing list [6] and Outages mailing list [7] often post about Internet outages. Recent work has shown the potential of using these lists to identify well-known Internet outages [8]. In addition, several power companies provide a live visualization of customers affected by power outages in areas they serve. We are scraping power outage data from the top 10 power companies in the U.S., and are in the process of curating a dataset of known power outages in different geographical areas.

Further, we will evaluate IODA’s macroscopic Internet-edge outages by cross-validating against outages detected by other state-of-the-art Internet-edge outage detection techniques. Several other research efforts, such as ISI’s Trinocular system [9] and the University of Maryland’s
Thunderping system [10], measure Internet-edge outages and make their data available to other researchers. By comparing IODA’s outage events with events detected by these systems, we will validate outages found by all of these techniques. This validation will help all of these systems, leading to improved outage detection accuracy for the state-of-the-art.

REFERENCES