I-seismograph: Observing, Measuring, and Analyzing Internet Earthquakes

Mingwei Zhang, Jun Li, and Scott Brooks
University of Oregon
Contact email: lijun@cs.uoregon.edu

***Abstract*—Disruptive events such as large-scale power outages, undersea cable cuts, or security attacks could have an impact on the Internet and cause the Internet to deviate from its normal state of operation, which we also refer to as an "Internet earthquake." As the Internet is a large, complex moving target, unfortunately little research has been done to define, observe, quantify and analyze such impact on the Internet, whether it is during a past event period or in real time. In this paper, we devise an Internet seismograph, or *I-seismograph*, to fill this gap. Since routing is the most basic function of the Internet and the Border Gateway Protocol (BGP) is the *de facto* standard inter-domain routing protocol, we focus on BGP to observe, measure, and analyze the Internet earthquakes. After defining what an impact to BGP entails, we describe how I-seismograph observes and measures the impact, exemplify its usage during both old and recent disruptive events, and further validate its accuracy and convergency. Finally, we show that I-seismograph can further be used to help analyze what happened to BGP while BGP experienced an impact, including which autonomous systems (AS) were affected most or which AS paths or path segments surged significantly in BGP updates during an Internet earthquake.**

***Index Terms*—Internet seismograph; Internet earthquake; Border Gateway Protocol (BGP); Autonomous System (AS)**

I. Introduction

The Internet has become a critical infrastructure of our society, yet few studies have focused on not only how to monitor the Internet as a whole, but also how to quantify the impact that disruptive events (such as [1], [2], [3], [4], [5], [6], [7]) may have on it. Although events such as security attacks, large-scale power outages, hurricanes, undersea cable cuts, and other types of natural disasters may cause observable disturbances to the normal operation of the Internet, we know little about the kind of impact each event might cause and how big it might be. The lack of such knowledge also makes it difficult to conduct effective network diagnosis, recovery, or other operation tasks. In fact, there is not even an established criterion for observing different kinds of impacts or for quantifying what "big" or "small" means.

This paper aims to fill this gap. We have designed an Internet seismograph, or *I-seismograph*, to measure "Internet earthquakes." It not only reports the magnitude of the impact (i.e., the Internet earthquake) during an event period, but also characterizes the nature of the impact. During a period when everything is normal, I-seismograph will simply report zero or close-to-zero impact; during a security attack, a natural disaster, or some other large-scale incident, if the regular operations of the Internet go awry, it can then indicate how badly the Internet was impacted. Not only can we use I-seismograph to measure the impact over a period in the past when an event is suspected to have affected the Internet, we also can use it to observe and measure an Internet earthquake in real time.

The main design idea of I-seismograph hinges upon discovering the "normal" state of the Internet, and then monitoring a given period to measure how the Internet activity deviates from it. Since routing is the most basic function on the Internet and the Border Gateway Protocol (BGP) is the *de facto* standard inter-domain routing protocol, our approach uses BGP data to discover the normal and abnormal states. This presents a challenge since BGP is very dynamic and BGP data are full of outliers. Furthermore, BGP has evolved greatly over the years and the definition of what is normal is ever-changing. To handle this dynamic nature, we have designed a two-phase clustering method that can discover what is normal and what is abnormal over a wide time span.

In addition to measuring and reporting the impact on BGP during an arbitrary monitoring period, I-seismograph can further be used to help analyze and diagnose what happened to BGP while BGP experiences an impact. Note that while an impact received by BGP during an event is not necessarily caused by the event, I-seismograph can still help network diagnosis and answer questions related to BGP itself. In particular, I-seismograph can help isolate abnormalities within BGP data, enabling the comparison between abnormal and normal BGP data and answering network diagnosis questions related to an Internet earthquake such as which autonomous systems (ASes) on the Internet have the largest number of affected IP prefixes, which ASes initiated the largest increase in BGP updates, or which AS paths or AS path segments surged most significantly in BGP updates.

In this paper, we first present our definition of impact on BGP (Sec. II) and describe how I-seismograph addresses various challenges in order to measure the impact that BGP receives during any period (Sec. III), followed by the validation of I-seismograph to ensure it possesses some key properties (Sec. IV). We then show the results when using I-

This material is based upon work partially supported by the USA National Science Foundation under Grant No. 0520326. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NSF.

seismograph against a set of old and recent events (Sec. V). Furthermore, we illustrate how I-seismograph can be used to help analyze what happened to BGP during an Internet earthquake (Sec. VI), and present I-seismograph running in real time online (Sec. VII). We then show I-seismograph is clearly different from the related work (Sec. VIII) and conclude this work (Sec. IX).

II. Defining Impact

We define an impact on BGP as any deviation from BGP's normal profile. The deviation consists of a *magnitude* and a *direction*. Assume we use a set of n distinct BGP attributes to inspect BGP, A_1, A_2, $\cdots$, A_n. Also assume we have defined a normal profile of BGP by identifying the normal values of those attributes. At any time t, if the values of these attributes of BGP are $a_1(t)$, $a_2(t)$, $\cdots$, $a_n(t)$, and they deviate from the normal profile as $\delta_1(t)$, $\delta_2(t)$, $\cdots$, $\delta_n(t)$, the impact that BGP receives at t is then a vector as follows: $i(t) =< \delta_1(t), \delta_2(t), ..., \delta_n(t) >$.

When looking at the impact on BGP over a time window, such as during the period of an event, we can define the impact during this window, say $[t_1, t_2]$, as: $I(t_1, t_2) = \int_{t_1}^{t_2} i(t)dt$ or $\sum_{t_1}^{t_2} i(t)$, depending on whether $i(t)$ is continuous or discrete.

III. Design of I-seismograph

Having defined BGP impact as a deviation from the normal profile of BGP, we now describe how we design I-seismograph to measure it.

A. Requirements and Challenges

I-seismograph must be correct. Specifically, while it must collect and process a very large amount of BGP data, it must identify a collection of BGP data that can accurately represent the normal profile of BGP, and for any monitoring period, if any BGP data in that period deviates from the normal profile of BGP, it must accurately derive the deviation of the BGP data from the normal profile. In doing so, it must consider both the spatial and temporal aspects of BGP. Spatially, BGP is a complex routing protocol concerning IP prefixes from the entire IP address space and involving BGP routers from all over the Internet. Temporally, the BGP protocol is constantly evolving to accommodate the growth and changes of the Internet; accordingly, what is considered normal at one time may be abnormal at another time (and vice versa). For example, at one point many pathological updates (such as duplicate withdrawals) existed on the Internet, but they have become much fewer over the years, while the forwarding dynamics have become more dominant [8].

I-seismograph must not only be easy to use, but it should also be flexible enough to allow for the impact calculation for any given period. It should be able to calculate the impact during a historical event, as well as the impact that BGP is currently experiencing.

Further, I-seismograph must be stable and reliable. Once it has sampled *enough* BGP data from different periods, the definition of the normal profile of BGP should converge to a stable state and I-seismograph should output the same impact results for a given period.

Last, it is desirable for I-seismograph to be informative toward understanding and handling Internet earthquakes. For any monitoring period during which an impact is observed, I-seismograph should be able to provide data that reflect BGP's deviation from normalcy and allow users and network operators to inspect the technology and operation details and effectively respond to the impact observed.

B. Methodology Overview

I-seismograph's basic data processing unit is BGP *databin*, which is simply a summary of the values of a set of distinct BGP attributes over a period of one minute.

To measure the impact during a monitoring period, our basic idea is to check every databin from that period, and see whether it is associated with a **normal cluster** composed of a set of normal databins, or an **abnormal cluster** composed of a set of abnormal databins. At any point there is only one normal cluster but there can be multiple abnormal clusters. The normal cluster represents the normalcy of BGP, and the abnormal clusters represent different types of BGP abnormalities. Once we know the associated cluster of every databin from a period, we then can calculate the impact of the databin as well as the impact during the entire period.

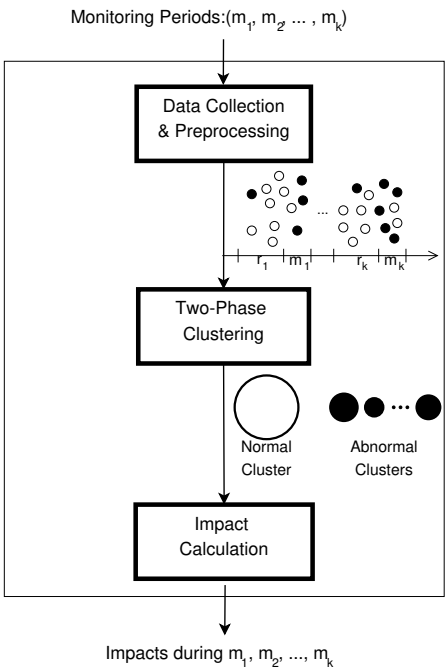
I-seismograph employs two different modes for measuring BGP impact: the heavyweight mode and the lightweight mode, which are depicted in Figs. 1(a) and 1(b), respectively. The latter requires that the normal and abnormal clusters be known *a priori*, while the former uses an unsupervised method to discover them automatically.

Both modes include a *Data Collection and Preprocessing* component to collect BGP data and pre-processes them into distinct databins, and an *Impact Calculation* component that uses the normal and abnormal clusters to calculate the impact of every databin and therefore the impact curve during monitoring periods. In addition, the heavyweight mode also includes a *Two-Phase Clustering Process* that discovers the databins which make up the normal cluster, and discovers abnormal databins and groups them into one or multiple abnormal clusters according to their similarity.

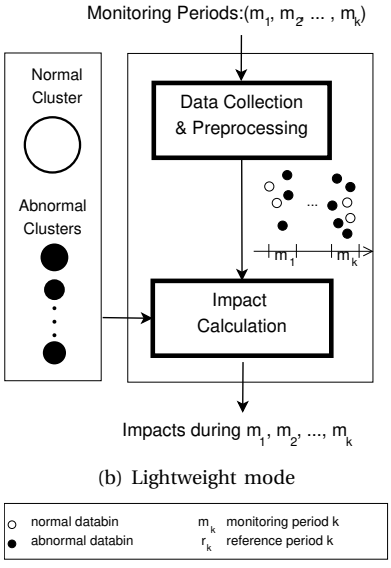
The lightweight mode is suitable for real-time Internet earthquake monitoring, or quickly checking the impact on BGP during a given period. The heavyweight mode is slower, but can be used to generate the normal and abnormal clusters needed by the lightweight mode.

C. Data Collection and Preprocessing

1) Data Collection and Cleaning: We collect BGP data from two types of periods: *monitoring periods* and *reference periods*. A monitoring period is a time window for which we want to measure the impact on BGP. It can be an arbitrary period, say $[T_1, T_2]$, that we want to monitor; or, to monitor



(a) Heavyweight mode



(b) Lightweight mode

Fig. 1: Two modes of I-seismograph.

BGP during an event that occurred from time t_1 to t_2, the monitoring period may be $[T_1, T_2]$, where $T_1 \le t_1 \le t_2 \le T_2$ (as we often do not know the accurate values of t_1 and t_2, the monitoring period can be noticeably larger than the real duration of an event).

Every monitoring period is associated with a reference period, which, as we will see later, provides reference data to help normalize BGP data and run the two-phase clustering process. Every reference period, when chosen, must have two properties: (1) adjacency to its associated monitoring period; and (2) sufficient length (such as four weeks). Because of these two properties, the majority of data in the reference period reflect what is normal for the particular monitoring period in question, which we define as short-term normal later in Sec. III-E. Note that we do not require a reference period to be free of anomalies, which is neither necessary nor practical to achieve. The fact is, even if it contains outliers and BGP data that are not (short-term) normal, because the period is long, the portion of such data should be small, and it will not affect the entire two-phase clustering process (Sec. III-E) of I-seismograph that eventually will only put normal data into the normal cluster.

Attribute	Description
Announcement	# of BGP announcements
Withdrawal	# of BGP withdrawals
Update	# of BGP updates
WADiff	# of new-path announcements after withdrawing an old path to the same IP prefix
AADiff	# of new-path announcements to the same IP prefix (thus implicit withdrawals)
WWDup	# of duplicate withdrawals to the same IP prefix
AADupType1	# of duplicate announcements to the same IP prefix where all fields of the announcements are unchanged
AADupType2	# of duplicate announcements to the same IP prefix where only the AS-PATH and NEXT-HOP fields of the announcements are the same
WADup	# of re-announcements after withdrawing the same path
AW	# of withdrawals after announcing the same path

TABLE I: Names and descriptions of selected BGP attributes.

The BGP data we collect are BGP updates, which are the conversation records between BGP routers, and which serve as firsthand data about BGP. We collect BGP updates from RIPE [9] and RouteViews [10]. These two organizations each maintain about 20 BGP collectors, and every collector peers with a number of BGP routers, also called *BGP peers*, to receive BGP updates; we use all available collectors and their peers. We then clean the updates by applying the algorithm described in [11] to remove those caused by session resets between a BGP collector and its peers.

2) Data Organization: With the BGP updates from a given period, we convert them minute by minute into BGP databins (Appendix B). Because an impact on BGP is about BGP deviating from its normalcy and thus will affect the dynamics of BGP, we choose every databin's attributes to be those that reflect the dynamics of BGP. Based on previous studies on BGP instability and dynamics, including those from [8], [12], we have identified ten distinct BGP attributes to summarize every minute of BGP activities (Table I).

3) Data Normalization: To discover the normal profile and different abnormal profiles of BGP, the data collected for this study will span a long period (the experiments that we report in Sec. V involve BGP data over 16 years). On one hand, we must ensure all BGP databins are comparable to each other; on the other hand, BGP is known to be evolving over time. Therefore, we must normalize the databins.

Our basic idea in normalizing any given databin is to find the *baseline* value of every attribute of the databin, and then use the ratio of the original value of the attribute versus its baseline value as the normalized value of the attribute.

To find the baseline value for every attribute of a databin, our first step is to find a set of *reference databins* for the databin in question. These reference databins will always be selected from a reference period, whether the databin being normalized is from a monitoring period or its associated

reference period. We run the K-Medoids (PAM) clustering algorithm to partition all the databins from the reference period into two clusters, and remove the databins from the cluster that is smaller—i.e., outliers. Then with the remaining databins—i.e., those belonging to the bigger cluster, we choose those databins that are of the same minute of the day as the databin in question to serve as the reference databins. As the reference databins are from the reference period and hence their values are comparable to the databin to normalize, we simply calculate the median of each attribute of all the reference databins, and use that as the baseline value for the attribute of the databin to normalize.

D. Impact Calculation

I-seismograph calculates impact from two levels: the impact of a single databin, and the impact during a monitoring period. Its input includes a normal cluster and multiple abnormal clusters. (We describe how we obtain these clusters in Sec. III-E.) The impact of an individual databin is based on the databin's relation with the normal cluster. The impact during a monitoring period checks how all the databins from the period deviate from the normal cluster collectively.

Every databin from a monitoring period will be assigned into either the normal cluster or one of the abnormal clusters. In the lightweight mode, the procedure is straightforward: with the normal and abnormal clusters as input, I-seismograph compares every databin's distance to the medoid of every cluster—i.e., the most centrally located databin in that cluster—and assigns the databin to the cluster with the nearest medoid. In the heavyweight mode, this is achieved through the two-phase clustering which we describe in Sec. III-E.

We introduce the following concepts to measure the impact of a databin and the impact during a monitoring period:

- **Impact value (of a databin $d =< d_1, d_2, \cdots, d_n >$).** This measures the *distance* of a databin from the normal. (We define every databin in the normal cluster to have an impact value of 0, and here we focus on those not in the normal cluster.) Since every databin is a vector with multiple basically orthogonal BGP attributes, we obtain its deviation distance along each attribute, and use the sum of all the deviation distances (i.e., the databin's Manhattan distance from the normal) as the value of the impact. We take the following steps: (1) For every attribute A_i ($i = 1, 2, ..., n$) of d, we use all the databins from the normal cluster to determine the mean μ_i and standard deviation σ_i of A_i. (2) We then calculate the databin's deviation distance from the normal along each attribute, denoted as δ_i ($i = 1, 2, ..., n$). With the databins in the normal clusters are mostly within $[\mu_i - \sigma_i, \mu_i + \sigma_i]$ (for more information see Appendix E), δ_i is $d_i - (\mu_i + \sigma_i)$ if $d_i > (\mu_i + \sigma_i)$, or $(\mu_i - \sigma_i) - d_i$ if $d_i < (\mu_i - \sigma_i)$, or 0 if $(\mu_i - \sigma_i) \leq d_i \leq (\mu_i + \sigma_i)$. (3) We normalize δ_i to be in the range of [0, 1] by dividing it by the maximum recorded value of δ_i. In the following, δ_i always refers to a normalized value. (4) Finally, we use the sum of the differences for all attributes, i.e., $\sum_{i=1}^{n} \delta_i$, as the distance of d from the normal. Since our study currently uses exactly 10 BGP attributes, every impact value will thus be between 0 and 10.
- **Impact direction (of a databin).** Every databin is a vector with multiple BGP attributes and may deviate from the normal along a specific direction. The impact direction of a databin indicates in which direction the databin deviates from the normal. Following the discussion of impact value above and using the same notations, we define the impact direction of a databin using the deviation vector $< \delta_1, \delta_2, \cdots, \delta_n >$.
- **Impact curve (of a monitoring period).** This is the plot of the impact values of all the databins from a monitoring period over time.
- **Dominant and peak impact directions (of a monitoring period).** The abnormal cluster that has more databins from the monitoring period than any other abnormal clusters is what we call the *dominant abnormal cluster* for the period. We define the impact direction of this cluster's medoid (i.e., its most centrally located databin) as the *dominant impact direction* for the monitoring period in question. In addition, we define the impact directions of those databins from a monitoring period that have a peak impact value as the *peak impact directions* of the period. Note that those databins may or may *not* belong to the dominant abnormal cluster. The dominant direction represents the overall trend during a monitoring period, and the peak direction indicates the behavior during the maximum impact.

E. Two-Phase Clustering Process

I-seismograph in heavyweight mode includes a two-phase clustering process to discover a normal cluster of normal databins and multiple abnormal clusters of abnormal databins. As shown in Fig. 1(a), the input to this process is composed of BGP databins from one or multiple monitoring periods and BGP databins from the reference period associated with each monitoring period, as described in Sec. III-C1.

The two-phase clustering is based on our concept of two-level normality: **short-term normal**, or **s-normal**; and **long-term normal**, or **l-normal**. S-normal refers to what is normal during a specific monitoring period and its associated reference period. L-normal refers to what is normal during a much longer period. Similarly, we use **s-abnormal** and **l-abnormal** to mean short-term and long-term abnormal, respectively. As such, the two-phase clustering process will take databins as input from multiple monitoring periods and their associated reference periods—which altogether spread over a long period, and process them in two different phases: **short-term clustering** and **long-term clustering**.

The short-term clustering serves as a filtering process; by discarding certain databins, it will ensure that every databin from a reference period is s-normal, whereas none of the databins from a monitoring period are. The long-term clustering then takes the result from the short-term

clustering as its input, and clusters all the databins; it will discover databins that are l-normal and those that are not, and group them based on their similarity into the normal cluster and multiple abnormal clusters, respectively. Below we describe each phase in detail.

1) Short-Term Clustering Phase: We take two steps in processing the databins from a monitoring period and its associated reference period: first, we process databins from the reference period; second, we use the result to help process databins from the monitoring period.

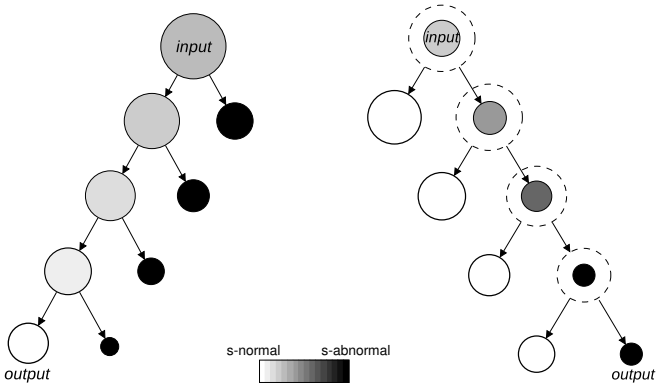
Processing Databins from Reference Period: Assuming a reference period spans over multiple days, for each day of databins, we run a clustering algorithm, which we call **N-clustering**, to see if it generates an s-normal cluster that contains only s-normal databins. If it does, we retain databins from the s-normal cluster and discard all other databins; otherwise, we discard the entire day (for more information see Appendix F).

N-clustering is a divisive hierarchical clustering algorithm [13]. It relies on two rules: the majority rule and the tightness rule. It assumes that the s-normal cluster—if it ever exists—must consist of more than 50% of the databins from the initial input, and these databins must be tightly clustered.

As shown in Fig. 2(a), N-clustering works as follows: (1) It begins with all the input databins as the root cluster, and uses K-Medoids to recursively split a cluster into two child clusters. K-Medoids is used because it creates non-overlapping clusters and is more resilient to outliers than other clustering algorithms such as K-Means. (2) Upon every split, it discards the smaller child because it has less than 50% of the databins and cannot be, or lead to, an s-normal cluster. (3) If the bigger child meets both the majority rule and the tightness rule, it is exactly the s-normal cluster to generate! If it meets the majority rule but not the tightness rule, it will be split again. If it does not meet the majority rule, however, no s-normal cluster will be found and N-clustering simply stops.

To determine whether a cluster is tight, we check its intra-distance and inter-distance [14]. The intra-distance shows how far apart databins within a cluster are, and the inter-distance is the distance between a cluster and its sibling cluster. When the intra- and inter-distance of a cluster reaches a *knee* or inflection point, we determine that this cluster is tight and does not need to be further split. (We choose 20% as the knee since the knee typically occurs when the intra-distance becomes no more than 20% of the inter-distance (Appendix C).)

Processing Databins from Monitoring Period: Now that databins from the reference period are all s-normal, we further process the databins from the monitoring period to only retain those that are s-abnormal. However, doing so is more difficult than retaining s-normal databins from the reference period. In the latter, every time we split a cluster of databins into two child clusters, we can discard the smaller child since this child is guaranteed not to contain s-normal databins. Now, because the majority databins from the monitoring period could be either s-normal or s-abnormal, if we run a clustering algorithm to split databins from the monitoring period, we do not know between the bigger and the smaller child clusters, which one to discard and which to further inspect.



(a) N-clustering for processing databins from a *reference* period

(b) A-clustering for processing databins from a *monitoring* period

Fig. 2: Short-term clustering. (Each circle represents a cluster, the dashed circle represents an inflated cluster, and a cluster with darker shade contains a higher percentage of s-abnormal databins.)

We overcome this difficulty by designing a new clustering algorithm, which we call **A-clustering**, to discover a cluster of s-abnormal databins (Fig 2(b)). Like N-clustering, it is also a divisive hierarchical clustering algorithm. It begins with one initial cluster with all the databins from the monitoring period, and also uses K-Medoids to split a cluster into two new child clusters. But, every time we split a cluster we inflate it with s-normal reference databins obtained earlier! Specifically, every time we split a cluster with n databins, including the very initial cluster, we randomly choose more than n s-normal reference databins and inject them to the cluster to create an inflated cluster. The inflated cluster will thus have a key property: *Its s-normal databins are the majority, and the s-abnormal databins to discover are the minority.* The majority here includes not only the injected, s-normal databins, but also those from the monitoring period that are also s-normal. As a result, after a binary split of the inflated cluster, we will be certain that the s-abnormal databins will go to the smaller child. The bigger child will not only include injected, s-normal databins, but will also act like a sticking ball to pick up as many s-normal databins as possible from the monitoring period. If the bigger child cannot pick up any s-normal databins from the monitoring period, the smaller child is already a cluster with all the s-abnormal databins and we are done; otherwise, we can continue to split the smaller child—again with s-normal reference databins injected first—until we finally find a child cluster with only s-abnormal databins.

2) Long-Term Clustering Phase: After we use short-term clustering to filter the databins for every monitoring period and its associated reference period, we can compare the databins from a monitoring period and those from its associated reference period, and see how abnormal the former are compared to the latter. However, such abnormality is

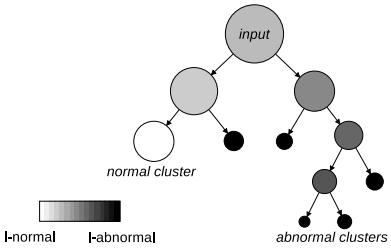


Fig. 3: Long-term clustering. (Its input is the output from the short-term clustering, and its output are the normal cluster and multiple abnormal clusters (5 in this figure)).

based on the short-term normality, and will not indicate the impact during a monitoring period over a long term. It is also hard to compare the impact from different monitoring periods that may be far from each other.

To address this limitation, we introduce the long-term clustering phase to derive the long-term normality, discover how abnormal the databins from different monitoring periods are from a long-term perspective, and group databins according to their long-term normality as well as long-term abnormality. The long-term clustering enables us to discover a common, long-term normality of BGP, and compare the impact from all the monitoring periods in the same context.

Like our two short-term clustering algorithms, the long-term clustering algorithm is also a divisive hierarchical clustering algorithm. As shown in Fig. 3, it will generate a normal cluster of long-term normal databins *and* multiple abnormal clusters of long-term abnormal databins. The initial input is a root cluster of all the s-abnormal and s-normal databins from multiple pairs of monitoring and reference periods. Every time we process a cluster, including the root cluster, we first check whether the cluster is tight by calculating its intra-distance, and compare it with the intra-distance of its parent cluster. If the two intra-distances differ by less than 1%, i.e., clustering helps little in further packing databins in this cluster, the cluster is tight (Appendix D), and it is a leaf cluster and we do not split it. Otherwise, we continue to use K-Medoids to split it into two child clusters. We then begin processing *every* child cluster, following the same procedure just mentioned. This recursive procedure will eventually stop, creating a tree of clusters. The largest leaf cluster is then the normal cluster; other leaf clusters are various abnormal clusters.

IV. Validating I-seismograph

In this section we validate I-seismograph. In particular, we investigate its convergency with more data input and its sensitivity to data sources, both along three key metrics. We demonstrate I-seismograph converges when more BGP data are used and it can derive similar results whether it uses RouteViews collectors or RIPE collectors. We compare its heavyweight mode against its lightweight mode in the next section (Sec. V-D) to show that I-seismograph obtains equivalent results no matter which mode it uses.

A. Metrics for Validating I-seismograph

In order to validate if I-seismograph produces similar results when different amount of input data are used or when different data sources are adopted. We use the following three metrics to compare the results from two different runs of I-seismograph:

- *Normal cluster difference*. Assuming the two normal clusters derived from two different runs of I-seismograph are N and N', their difference is the difference of the medoid databin of N and that of N', which is the sum of absolute differences along all BGP attributes.
- *Impact curve difference*. Assuming the impact curves for a monitoring period $[t_1, t_2]$ are $i(t)$ and $i'(t)$ from two different runs of I-seismograph, their difference is $\int_{t_1}^{t_2} |i'(t) - i(t)|$.
- *Dominant impact direction difference*. Assuming the dominant impact directions for a monitoring period $[t_1, t_2]$ are d and d' from two different runs of I-seismograph, their difference is the sum of d and d''s absolute differences along all attributes.

B. Convergency

A key property that I-seismograph must possess is that it must converge with more data input. Specifically, with enough data input, I-seismograph should (1) produce a normal cluster that defines a stable and reliable normalcy of BGP; and (2) report consistent impact results for any monitoring period. We design an iterative procedure to evaluate I-seismograph's convergency as follows.

1) We select 16 different monitoring periods and their associated reference periods from 2001 to 2016 as input, and a specific target period M that we run I-seismograph as below to monitor. Pick n random permutations of all 16 monitoring periods and repeat Steps 2) and 3) below for every permutation.

2) Denote the current permutation $m_{x1}, m_{x2}, \cdots, m_{x16}$. Run I-seismograph in the heavyweight mode 16 times, each time independently measuring the impact over the target period M. In the first time use BGP data from m_{x1} and its associated reference period as the only input, then every following time add the next monitoring period in sequence, until the last time that includes all 16 monitoring periods.

3) Each time after adding a monitoring period, compare the results from I-seismograph in terms of the three metrics defined in Sec. IV-A, and record the difference.

4) Gather all the stepwise convergency check results from 3) and conduct the statistical analysis to verify if I-seismograph converges.

Fig 4 shows how I-seismograph converges along the three metrics with n=40 (results are similar for all n>10). Clearly, as more monitoring periods are added, i.e., as more data are provided as input to I-seismograph, results of all three metrics approach 0. Specifically, the definition of the normalcy of BGP, as represented by the normal cluster, will become fairly stable when enough input is used. In other words, the normal cluster will be approximately the same

so long as BGP data from enough periods are fed to I-seismograph. Similarly, both impact curves and dominant impact directions also converge, reaching stable results as enough data are used. (More information can be found in Appendix G)

C. Sensitivity to Data Sources

I-seismograph currently relies on BGP collectors from RouteViews and RIPE to gather BGP updates as its input (Appendix A). These collectors are in different locations on the Internet and peer with different BGP routers, i.e., BGP peers. However, as every BGP router on the Internet strives to keep their routes to every IP address up-to-date, we found that in most cases the BGP dynamics that can be heard by RouteViews peers can also be heard by RIPE peers, and vice versa. (In fact, all 16 events that we report in Sec. V are heard by both RouteViews and RIPE.) In this subsection we therefore investigate whether I-seismograph will derive similar normal clusters and impact results, no matter whether it uses RouteViews or RIPE collectors.

We compare I-seismograph using RouteViews with I-seismograph using RIPE, again along the three metrics from Sec. IV-A. We randomly pick from RouteViews and RIPE j collectors each, with j=1, 2, ..., 11. For each value of j, we run I-seismograph with either j RouteViews collectors or j RIPE collectors. In each run we choose 4 one-month periods from each year from 2008 to 2017, i.e., totally 40 periods, in order to obtain the normal cluster and derive the impact curve and dominant impact direction over a target two-day monitoring period. Here, for every j, we will use 10 different choices of j collectors in order to collect statistically meaningful results. Also note RouteViews and RIPE can both have at most 11 collectors that exist from 2008 to 2017.

We therefore can compare for each value of j (j=1, 2, ..., 11) how I-seismograph performs when different data sources are used. Fig. 4 shows the results with RouteViews only differ very little from those with RIPE. In particular, while the normal cluster difference can be as high as 10, the median values are only 0.27 on average, with minimum and maximum respectively 0.23 and 0.31. Compared with the maximal possible difference of impact curves (28800), the impact curve difference values are all fairly minimal (Fig. 5(b)). The dominant impact direction difference is a bit high when only one collector is used (a bit over 1 out of the maximal value of 10), but they become quite low on average when more collectors are used (Fig. 5(c)).

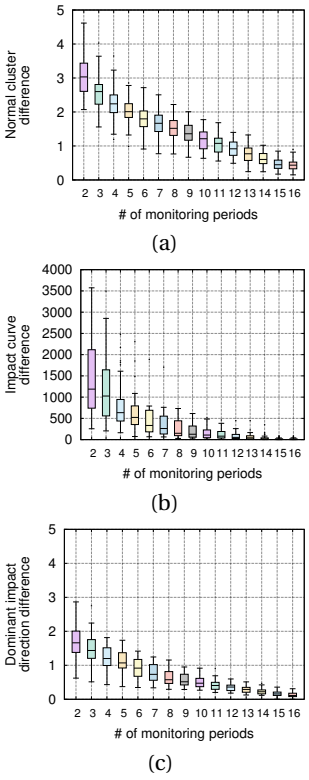


Fig. 4: I-seismograph convergency with more data input.

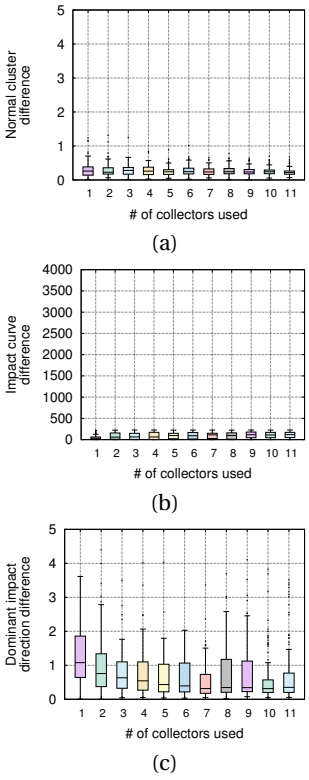


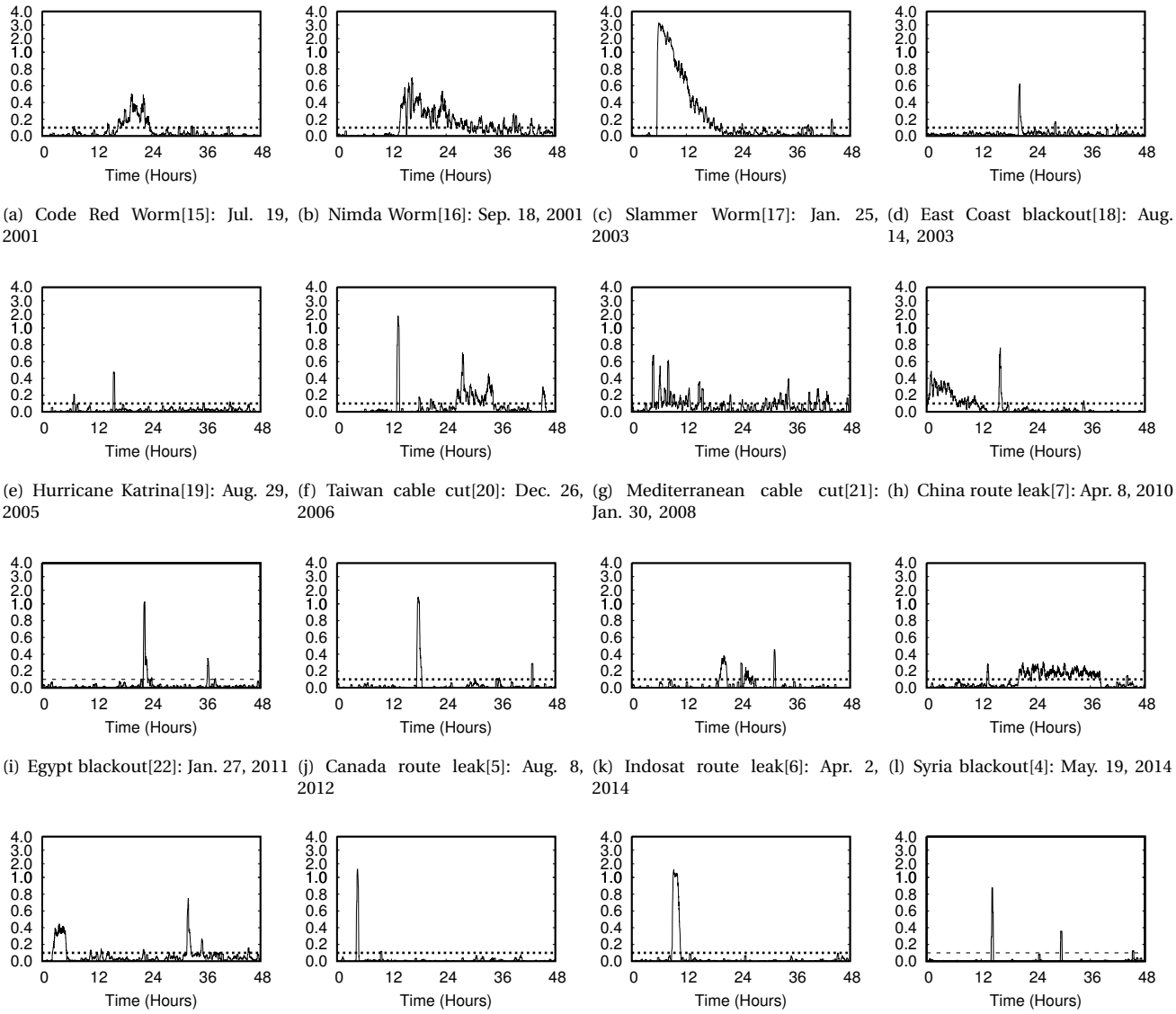
Fig. 5: I-seismograph sensitivity to data sources (RouteViews vs. RIPE).

V. Impact Results

In this section, we apply I-seismograph to measure the impact on BGP, i.e., the Internet earthquake. We select 16 monitoring periods from 2001 to 2016 (Sec. V-A), use the heavyweight mode with all 16 monitoring periods and their associated reference periods to derive the normal cluster, and measure the impact on BGP during each one of the 16 monitoring periods. Note that the impact that I-seismograph detects during each event is likely different, and an event may not even cause BGP to deviate from its normalcy (such as those that only affect a small region). We report and analyze the impact curves in Sec. V-B and impact directions in Sec. V-C, and verify in Sec. V-D that I-seismograph in the lightweight mode will produce similar impact results over all 16 monitoring periods.

A. Setup

We have identified a number of events to see if the normal operation of BGP was disrupted during an event. To demonstrate the efficacy of I-seismograph, we selected 16 events from a wide time span from 2001 to 2016. We associated every event with a two-day monitoring period during which the event occurred; a two-day time window is long enough to span the entire duration of each event, so when we monitor the impact during the two-day period, we can guarantee we will monitor the impact during the event. We further associated every event with a 4-week reference period that immediately precedes the monitoring period; doing so meets the two required properties for selecting the reference period in question, as described in Sec. III-C1. We thus used 2*24*60 databins from the event period and 4*7*24*60 databins from the reference period. Finally, we ran I-seismograph to report the impacts for each monitoring period, which extracts a databin to summarize the BGP data for every minute during the period and produces the impact results for the entire period as described in Sec. III-D.



(a) Code Red Worm[15]: Jul. 19, 2001 (b) Nimda Worm[16]: Sep. 18, 2001 (c) Slammer Worm[17]: Jan. 25, 2003 (d) East Coast blackout[18]: Aug. 14, 2003

(e) Hurricane Katrina[19]: Aug. 29, 2005 (f) Taiwan cable cut[20]: Dec. 26, 2006 (g) Mediterranean cable cut[21]: Jan. 30, 2008 (h) China route leak[7]: Apr. 8, 2010

(i) Egypt blackout[22]: Jan. 27, 2011 (j) Canada route leak[5]: Aug. 8, 2012 (k) Indosat route leak[6]: Apr. 2, 2014 (l) Syria blackout[4]: May. 19, 2014

(m) CISCO 512K router failure[23]: Aug. 13, 2014 (n) Time Warner blackout[3]: Aug. 27, 2014 (o) Malaysia route leak[2]: Jun. 12, 2015 (p) SEA-ME-WE-4 cable cut[24]: May. 17, 2016

Fig. 6: Impact curves during 16 different monitoring periods (with every period's starting date).

B. Impact Curves and Their Patterns

Fig. 6 presents the impact curves produced by I-seismograph over all 16 monitoring periods. These curves have various patterns. An impact curve often consists of one or multiple waves, where we define each wave to consist of an ascent followed by a descent. An ascent is the portion of the curve where the impact values climb to a peak value from the baseline, and a descent is the portion where the impact values decline to the baseline from the peak. We use an empirical value of 0.1 for the baseline as the impact values lower than 0.1 are negligible. We look at the impact patterns from the following perspectives:

- *Ascent of a wave.* The ascent pattern of a wave reflects how fast the impact on BGP reaches its height. The impact can reach a peak value almost instantly or slowly. Either way, it can reach the peak value with a monotonic increase, or up and down instead while the overall trend is still going up. The wave in the Slammer worm curve, for example, has a quickly rising ascent (Fig. 6(c)), whereas the wave in the Code Red worm curve has a slowly rising ascent (Fig. 6(a)). We can see that most ascents in Fig. 6, however, are fast-rising.
- *Descent of a wave.* Similarly, the impact can also decrease from a peak value to the baseline almost instantly or gradually, reflecting how quickly BGP returns to its normal status after an impact. It can subside from a peak value gradually over time, as shown in the Slammer worm curve (Fig. 6(c)), or quickly, as in the first wave of the Taiwan cable cut curve and the Malaysia route leak curve (Figs. 6(f) and 6(o), respectively). We can see in Fig. 6 that roughly half of the descents are fast, and half are slow. Here, if both the ascent and descent of a wave are

fast, the wave is then basically a spike.

- *Wave duration.* The impact on BGP during a wave can last a long time, or can be simply short-lived. A long-lived wave is often at least about half a day (e.g., Figs. 6(a), 6(c), 6(h), 6(l)), but could also last almost an entire monitoring period (e.g., Fig. 6(g)). A short-lived wave is typically a spike, whereas the spike may be of either a high value or a low value. From Fig. 6 we can see that seven out of 16 (i.e., about half) curves only contain spike waves (i.e., Figs. 6(d), 6(e), 6(i), 6(j), 6(n), 6(o), 6(p)).
- *Wave magnitude.* While the maximal value of an impact is 10 (Sec. III-D), out of 16 curves in Fig. 6 we see that for most curves, no wave has a peak value higher than 1.0. The exceptions are the curves for Slammer worm, the Taiwan cable cut, the Egypt blackout, the Canada route leak, the Time Warner outage, and the Malaysia route leak, where the impact value can be as high as 3.1, 1.9, 1.1, 1.5, 1.5, 1.5, respectively (Figs. 6(c), 6(f), 6(i), 6(j), 6(n), 6(o)).
- *Number of waves.* An impact curve during a monitoring period could experience just one wave (e.g., Fig. 6(c)), or multiple waves (e.g., Fig. 6(h)). As every wave contains a departure and then a return to the baseline, a higher number of waves can indicate a higher level of oscillation due to the impact on BGP during a monitoring period.
- *Interval between waves.* An interval between waves is a time window during which there is no noticeable impact on BGP. There can be either short intervals or long intervals between waves. If an interval is short, it means after the impact on BGP declines to the baseline, the BGP is going to experience yet another new wave of impact soon. For example, the Mediterranean cable cut curve has waves only minutes apart (Fig. 6(g)). On the contrary, a long interval indicates a long quiescent period without much impact on BGP. For instance, Fig. 6(m) has two distinct waves, where the first wave corresponds to an unreported event and the second wave coincides with the occurrence of the CISCO 512K router failure event. Because these two events are almost 26 hours apart and nothing disruptive happened between them, we can see a long interval of almost 26 hours between the two waves.

C. Impact Directions

Depending on which BGP attributes deviate from the normal state, receiving an impact is not necessarily a bad thing. For example, while a lot of WWDup is pathological, a higher number of BGP updates could simply mean BGP is doing its job. An impact direction can indicate which attributes deviate from the normal state. Some attributes (e.g., AADiff and WADiff) show forwarding dynamics of BGP that reflect topological changes, some (e.g., WWDup and AADupType1) show pathological behavior due to redundant updates, and some (e.g., WADup) could mean both. Readers can further refer to our earlier work [8] to see how we can analyze different BGP attributes to understand BGP dynamics (see Table I for attribute definitions).

The simplest method in understanding the impact directions during a monitoring period is to look at the dominant impact directions during the period. For the 16 monitoring periods from Fig. 6, Table II shows the common BGP attributes in dominant impact directions for the same type of monitoring periods. While they all show an increase in the amount of BGP announcements as well as updates, all blackout events went high on the amount of Withdrawal and WADiff, all cable cut events spiked on the amount of AW dynamics, all worm events jumped on AADiff dynamics, and all route leak events had outstanding values on AADiff and WADup. During a blackout many BGP routers will learn they no longer can reach prefixes from the blackout regions, causing a hike of Withdrawals to their neighbors; the neighbors may decide new paths to those prefixes and then announce them, also causing the hike of WADiff. During a cable cut, however, once a path is withdrawn, it is very likely that there will not be an alternate path, thus no announcement hikes, but simply many withdrawals corresponding to early announcements (thus AWs) that are sent to adjacent BGP routers regarding IP prefixes on the other side of the undersea cable. During a worm, when a link between two BGP routers is congested by a worm, both routers will treat the link as unavailable and directly send out announcements of new paths that will not use the link, thus causing many AADiffs. During a route leak, there will be many leaked announcements with incorrect paths to affected prefixes, thus causing many AADiffs; furthermore, the havoc can potentially cause many BGP routers to withdraw the paths to such prefixes, followed by the announcements from the origin ASes to re-establish the correct paths to the affected prefixes, further causing many WADups.

Event type	Common attributes in dominant impact directions
blackout	Announcement, Update, Withdrawal, WADiff
cable cut	Announcement, Update, AW
worm	Announcement, Update, AADiff
route leak	Announcement, Update, AADiff, WADup

TABLE II: Common BGP attributes in dominant impact directions for the same type of events.

Also interesting is the peak impact directions over these periods. These peak impact directions show the maximum impact during a period, and do not necessarily agree with the dominant impact direction. Some peaks simply show a higher level of benign forwarding dynamics (e.g., the peaks of the Code Red and Nimda worms, the Syria and East Coast blackout, the Malaysia and Indosat route leaks, the first peak of the Taiwan cable cut and the second peak of the Mediterranean cable cut, and the CISCO 512K router failure); some peaks show pathological behavior (e.g., the first peak of the CISCO router failure and the second peak of the Taiwan cable cut and the Indosat route leak); and some peaks show both (e.g., the peaks of the Slammer and Hurricane Katrina, the Canada and China route leak, and TimeWarner outage).

D. Heavyweight Mode vs. Lightweight Mode

If I-seismograph works correctly, it should generate equivalent impact results whether it is used in the heavy-

weight mode or the lightweight mode. In Secs. V-B and V-C we have shown impact results under the heavyweight mode for the 16 different monitoring periods. In this section, we verify I-seismograph in the lightweight mode will produce similar impact results over the same 16 monitoring periods. For each monitoring period we compare, we first use the other 15 monitoring periods as the input to I-seismograph and run I-seismograph in the heavyweight mode to generate the normal cluster and abnormal clusters. We then run I-seismograph in the lightweight mode to obtain the impact curves and dominant impact directions for each monitoring period.

Monitoring Period	Impact Curve Difference per Databin		Dominant Impact Direction Difference
	average	maximum	
Code Red worm[15]	0.000360	0.099792	0.550326
Nimda worm[16]	0.000866	0.172153	0.171812
Slammer worm[17]	0.145369	2.871274	1.470100
East coast blackout[18]	0.001174	0.052728	0.185583
Hurricane Katrina[19]	0.000066	0.021473	0.820372
Taiwan cable cut[20]	0.001779	0.147421	0.253638
Mediterranean cable cut[21]	0.000490	0.147288	0.374698
China route leak[7]	0.000243	0.075015	0.014345
Egypt blackout[22]	0.000667	0.317839	0.131542
Canada route leak[5]	0.000108	0.015956	0.031874
Indosat route leak[6]	0.000434	0.035109	0.382370
Syria blackout[4]	0.000304	0.081255	0.111283
CISCO 512K router failure[23]	0.000132	0.019330	0.737440
Time Warner blackout[3]	0.000629	0.152325	0.408921
Malaysia route leak[2]	0.008808	0.091440	0.041744
SEA-ME-WE-4 cable cut[24]	0.000156	0.032317	0.009128
average:	0.010099	0.270795	0.293449

TABLE III: Difference between running I-seismograph in heavyweight and lightweight mode. The maximum value for each difference value is 10.

Table III shows the impact curve difference per databin and the dominant impact direction difference for each monitoring period between the two modes. Clearly, while the highest possible value is 10 for all differences, both the average differences and the maximum differences of impact per databin are insignificant (their averages over all the monitoring periods are only 0.0101 and 0.271, respectively), and dominant impact directions for each period between two modes also only differ 0.293 on average.

From these results we can see that we can feed past BGP data into the heavyweight mode to generate normal and abnormal clusters, and then switch to the lightweight mode to more easily and quickly measure impacts for future monitoring periods, including real-time monitoring. Of course we can also add new, more up-to-date BGP data to the heavyweight mode at any time to update the normal and abnormal clusters, making the future impact measurement more accurate. Meanwhile, as the correctness of the lightweight mode hinges upon the correctness of the normal and abnormal clusters generated from the heavyweight mode, the result above also demonstrates that the heavyweight mode is good at discovering and distinguishing the normal and the abnormal.

VI. Further Analysis: What Happened to BGP in an Internet Earthquake?

In addition to measuring and reporting the impact on BGP during a monitoring period, I-seismograph can further be used to help analyze what happened to BGP during the impact. Note that receiving an impact during an event does not necessarily mean that the impact is caused by the event. There could be other things happening simultaneously that cause the impact (for example, an impact spike during a regional blackout could actually be caused by an unknown large-scale route leak).

In this section, we focus on analyzing the following two questions that frequently arise in network diagnosis:

1) **Origin AS analysis**: During an Internet earthquake, which ASes on the Internet are affected most in terms of having the largest increase of BGP updates originated from these ASes? A similar but different question is, which ASes are affected most in terms of having the largest number of IP prefixes affected? (A prefix is "affected" if it is announced or updated more frequently than usual.)
2) **AS path analysis**: During an Internet earthquake, among all the AS paths or AS path segments that appear in BGP updates, which AS paths or AS path segments surged most significantly?

Given the scale, complexity, and very distributed nature of Internet routing data, both questions above, in general, are difficult to answer. However, the design of I-seismograph provides an effective solution to both questions. Recall from Sec. III that I-seismograph can derive abnormal clusters which encompass abnormal databins and a normal cluster which includes all the databins representing what is "normal." We can therefore compare the databins from abnormal clusters against those from the normal cluster, and compare the BGP updates corresponding to these databins, in order to draw comparisons to answer the two above questions. We describe the details for both in the rest of this section.

A. Origin AS Analysis

Given that I-seismograph can separate databins into a normal cluster and abnormal clusters, we can take advantage of this separation to conduct the origin AS analysis, i.e., identify the top origin ASes that had the largest increase of originated BGP updates or largest number of affected IP prefixes. The procedure is as follows.

- *1)* First, by running I-seismograph for a monitoring period, we can generate one or multiple abnormal clusters. Note that here we can run I-seismograph either in the lightweight mode or in the heavyweight mode; if the former we already have a normal cluster, and if the latter we will generate a normal cluster as well.

- *2)* Second, we select databins of interest from the abnormal clusters. For example, we can choose all the databins from all the abnormal clusters to study the overall anomaly; we can choose the databins from only the dominant abnormal cluster in order to focus on the dominant impact direction; or we can choose the databins that represent the peak impact direction.
- *3)* Third, we randomly select the same number of databins from the normal cluster and use these databins as our reference of usual behavior of BGP. Note that every databin is a summary of BGP behavior for a one-minute window, and the total length of time of abnormal databins selected is thus equal to that of the normal databins selected, thus ensuring we compare the normal and abnormal BGP behavior over the same number of minutes.
- *4)* Fourth, we collect "abnormal" and "normal" BGP updates corresponding to the abnormal databins and the normal databins selected above, respectively, and identify the origin AS of every BGP update. Here, to identify the origin AS of a BGP update, one can look at the IP prefix of the update (sometimes an update may have more than one prefix) and determine the origin AS of the prefix. We currently use RIPE's *whois* database. We do not choose to use the first AS from the AS-path in the update as the originator of the prefix, mainly because the first AS, and sometimes even the entire AS-path, is not guaranteed to be authentic. This is particularly important given that in some disruptive events, such as route leaks, a misconfigured or malicious AS could be sending a very large number of BGP updates with incorrect origins and AS-paths. Also, if a BGP update is a withdrawal, it does not contain AS-path information.
- *5)* Finally, we can determine which ASes are affected most, either in terms of having the largest increase of BGP updates originated from these ASes, or in terms of having the largest number of IP prefixes affected. If the former, we can simply look at the total number of "abnormal" updates vs. "normal" updates from each AS, and determine which ASes have the largest increase of updates. If the latter, for every prefix of each AS, we can see if the prefix is affected with significantly more "abnormal" updates than "normal" updates for the prefix, count how many prefixes in each AS are affected, and determine which ASes have the largest number of IP prefixes affected. One could even combine traffic information regarding the affected ASes or prefixes (*if* such information is available), such as their inbound or outbound traffic volume, to further determine which ASes are affected most also in terms of their traffic.

As an example, we can conduct an origin AS analysis to investigate which ASes are affected the most during the Taiwan cable cut event [20]. Table IV shows the top-10 ASes with the largest increase of updates. We can see that corresponding to the databins from the abnormal clusters (column "Abn."), these ASes have 391 to 3304 updates, a great contrast against only at most 11 BGP updates associated with the normal cluster (column "Nor."). In fact, nine out of ten ASes do not even initiate BGP updates after they settled to normalcy. Also, from the table we can see that all top 10 ASes are from China, India, Indonesia, Philippines, and Singapore (column "Loc."), which all heavily used the Taiwan undersea cable to connect their prefixes to the outside across the Pacific Ocean. Users can thus identify not only the most affected ASes during a time window, but also approximately the affected geographic region (i.e., Eastern Asia in this case). Table V further shows the top-10 ASes with the largest number of prefixes (174 to 1254) affected during this event. It is worth noting that nine ASes appeared on the top ten list of both tables, even though the order of these ASes is not the same for the two tables. Furthermore, as an ISP may contain one or more ASes, we could derive the top ISPs with the largest increase of updates or largest number of prefixes affected during the event, as shown in the last column of Tables IV and V.

ASN	Nor.	Abn.	Loc.	ISP	Top ISPs
AS4134	0	3304	CN	China Telecom	China Telecom China Unicom TATA Comm. Sify Limited INDOSATM2 Smart Comm. StarHub
AS4755	11	1071	IN	TATA Comm.	
AS9583	0	940	IN	Sify Limited	
AS4812	0	841	CN	China Telecom	
AS4837	0	792	CN	China Unicom	
AS4795	0	514	ID	INDOSATM2	
AS17816	0	433	CN	China Unicom	
AS10139	0	401	PH	Smart Comm.	
AS4808	0	394	CN	China Unicom	
AS10091	0	391	SG	StarHub	

TABLE IV: Top 10 ASes with the largest increase of originated BGP updates during the Taiwan cable cut event.

ASN	Nor.	Abn.	Loc.	ISP	Top ISPs
AS4134	0	1254	CN	China Telecom	China Telecom China Unicom TATA Comm. Sify Limited Smart Comm. INDOSATM2 StarHub Wharf T&T
AS4755	2	564	IN	TATA Comm.	
AS4812	0	313	CN	China Telecom	
AS4808	0	300	CN	China Unicom	
AS9583	0	288	IN	Sify Limited	
AS4837	0	265	CN	China Unicom	
AS10139	0	259	PH	Smart Comm.	
AS4795	0	187	ID	INDOSATM2	
AS10091	0	177	SG	StarHub	
AS9381	0	174	HK	Wharf T&T	

TABLE V: Top 10 ASes with the largest number of prefixes affected during the Taiwan cable cut event.

Another example is the most affected ASes during the CISCO 512K router failure [23]. Different from the most affected ASes during the Taiwan undersea cable cut where these ASes are geographically concentrated, ASes affected by the CISCO 512K router failure are much more spread out over the entire Internet. This pattern is expected given the wide-spread nature of this event where the failure occurred in many areas. In fact, more ASes are affected during the CISCO 512K router failure than during the Taiwan cable cut; Fig. 7 shows during the CISCO 512K router failure how many more BGP updates are originated from top 100 most affected ASes and how many prefixes are affected from top 100 most affected ASes.

B. AS Path Analysis

In parallel to analyzing the origin ASes, it is also important to investigate the AS paths or AS path segments that

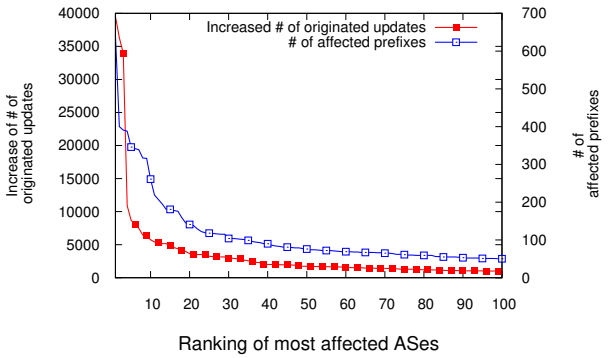


Fig. 7: The increased number of originated updates and the number of affected prefixes for ASes during CISCO 512K router failure event.

appear in BGP updates more frequently during an Internet earthquake, which we call AS path analysis. To conduct this analysis, we apply a procedure similar to that used in Sec. VI-A. The procedure is as follows.

- *1-3)* Same as Steps (1)–(3) for origin AS analysis as described in Sec. VI-A.
- *4)* Fourth, we collect "abnormal" and "normal" BGP updates corresponding to the abnormal databins and the normal databins selected above, respectively, and retrieve the AS path field of every BGP update. Here, every AS path may contain multiple AS path segments where each AS path segment can contain one AS, two ASes, or up to all consecutive ASes on the AS path.
- *5)* Fifth, we count and compare the total number of appearances of every AS path segment in "abnormal" updates and in "normal" updates. As a result, for each length, we learn which AS path segments of that length have the most increase of their number of appearances, indicating which segments surged most significantly in an Internet earthquake.
- *6)* Finally, we compare the lists of top AS path segments with different lengths to see which ASes or AS segments appeared across most or all lists, thus further revealing the ASes that are mostly likely related to an Internet earthquake.

We demonstrate the AS path analysis by examining the BGP dynamics resulting from the Canada route leak event in 2012 [5]. In this event, AS 46618 (Dery Telecom) falsely announced paths for 107,409 prefixes obtained from one of its providers AS 5769 (VIDEOTRON) to its other provider AS 577 (Bell); AS 577 then accepted all paths for the leaked prefixes and further propagated those paths into the Internet. By applying the aforementioned six-step AS path analysis procedure to this event, as shown in Fig. 8, we can derive three graphs comprising the 10 AS path segments with lengths of 4 ASes, 5 ASes, and 6 ASes, respectively, whose number of appearances surged most dramatically. The highlighted sequence of nodes appears in all three graphs, forming the path segment 3549–6453–577-46618–5769, while AS 3549 and AS 6453 are I-seismograph's vantage point AS and its provider. Since AS 577, AS 6453, and AS 5769 are directly involved in the route leak event, and the AS path segment 577–46618–5769 appeared in all of the leaked routes, the AS path analysis presented here shows that I-seismograph can indeed effectively identify which ASes and/or AS path segments are the source of an anomaly.

VII. Running I-seismograph

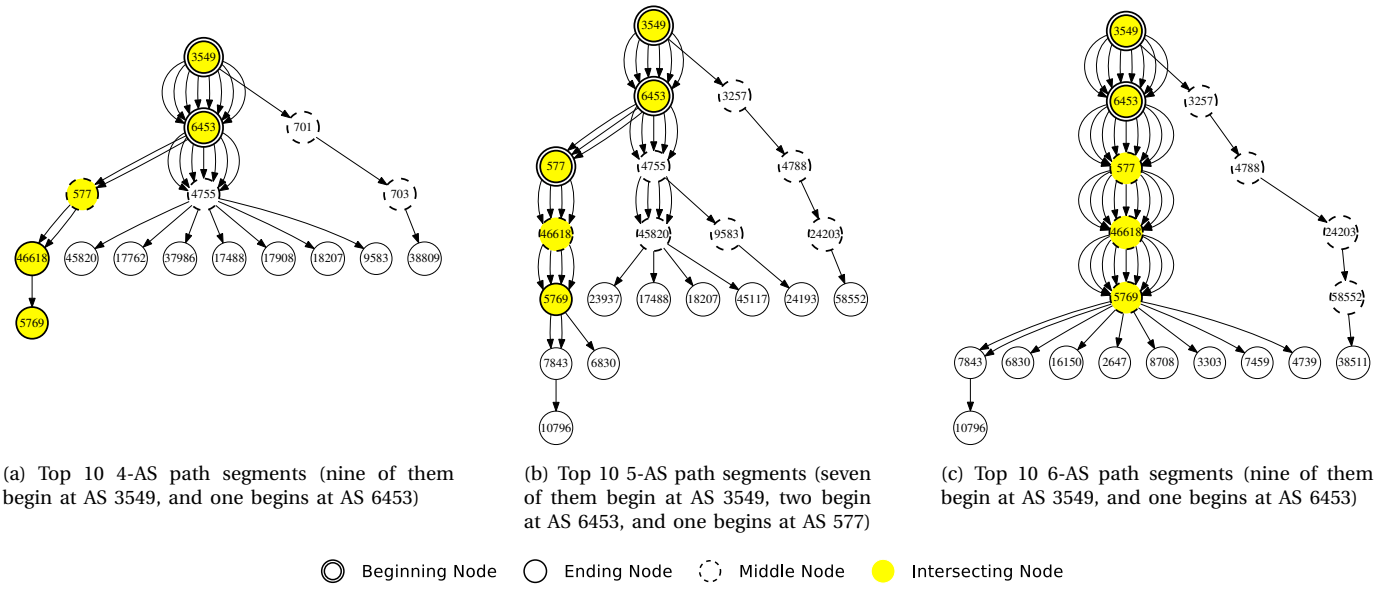
I-seismograph is easy to set up for real-time monitoring of Internet earthquakes, and its service can be made available through a website. We have implemented and deployed a real-time version of I-seismograph online at http://iseismograph.cs.uoregon.edu. It can run in the heavyweight mode offline and use historical BGP data to derive and update the long-term normalcy of BGP dynamics. Further, it can run in the lightweight mode and apply the long-term normalcy onto the BGP data to monitor the impact on BGP in real time. We optimized the implementation in order to achieve a near real-time data processing speed. For example, I-seismograph has multiple threads running in parallel, with one separate thread for each BGP peer that provides BGP data.

Data Sources. I-seismograph currently utilizes the BGP data collected from both RouteViews and RIPE. Note that while the data collectors of RouteViews and RIPE obtain new BGP data in real time, RouteViews' collectors only archive the data every 15 minutes and RIPE does so every 5 minutes, thus introducing a delay for 15 minutes and 5 minutes, respectively. We plan to incorporate more data sources in the future, including true real-time BGP update feeds such as those from BGPMon [25] and BGPStream [26].

Performance of I-seismograph. The performance of I-seismograph depends entirely on the mode of operation. When in lightweight mode, even on a laptop computer (Intel Core i5 @ 1.87 GHz, 8GB RAM), it takes less than a minute for I-seismograph to analyze the impact across a two-day period. In fact, the lightweight mode is perfectly suitable for running I-seismograph in real time. As soon as new BGP data become available, it only takes I-seismograph less than one second to parse a minute's worth of BGP data and produce monitoring results. I-seismograph in heavyweight mode would need much more time: approximately 25 minutes for each two-day period when processing a total of sixteen such periods simultaneously. However, I-seismograph in heavyweight mode can run offline, and need not be invoked often.

VIII. Related Work

Little research has been conducted to systematically define, detect and quantify how Internet routing may deviate at a large scale from its normal state of operation, i.e., Internet earthquake as we have referred to in this paper. Most closely related to our research are various studies that monitor, detect and analyze the extensive Internet routing dynamics and large-scale anomalies toward BGP, as well



(a) Top 10 4-AS path segments (nine of them begin at AS 3549, and one begins at AS 6453)

(b) Top 10 5-AS path segments (seven of them begin at AS 3549, two begin at AS 6453, and one begins at AS 577)

(c) Top 10 6-AS path segments (nine of them begin at AS 3549, and one begins at AS 6453)

Fig. 8: Top-10 AS path segments of different lengths during the Canada route leak. Every path segment has a beginning node, one or multiple middle nodes, and an ending node. Nodes highlighted are ASes (i.e., 3549, 6453, 577, 46618, 5769) that appear in all three graphs.

as some case studies that investigate the effects of various events on BGP. We discuss these related research efforts in this section, with a summary how our work differs from *recent* related studies.

Observing and assessing BGP dynamics at a large scale have been well studied [27]. Early work by Labovitz et al. [12] used archived BGP updates from route servers at major US network exchange points and found several unexpected trends in routing dynamics, with pathological duplicate BGP updates contributing to the majority of unstable dynamics. Li et al. [8] revisited BGP dynamics, a decade after the study in [12], and found that BGP dynamics became "busier" but "healthier" with much less pathological behavior. Elmokashfi et al. [28], [29] also studied the evolution of BGP dynamics over ten years, and found that the rate of BGP messages remained stable with respect to the size of the Internet AS-level topology, in line with the discoveries from Rexford et al. in 2002 [30]. There are also tools such as BGPfuse [31], BGPlay [32], iBGPlay [33], and Link-Rank [34] which visualize BGP dynamics. None of these studies or tools, however, can help quantify the extent to which the routing infrastructure, or BGP in particular, deviates from its normal state when certain dynamics occur. In fact, because most aforementioned BGP dynamics work focuses on a specific period, they do not even offer what the normal state might be in a long-term sense.

Aside from studies of the overall dynamics of BGP, there are also studies that focus on detecting BGP instabilities and anomalies [35]. Deshpande et al. [36] proposed an online instability detection architecture for routers, which employs statistical pattern recognition of BGP update volumes to detect BGP instabilities caused by accidental and malicious activities. Research in [37] applied wavelet analysis [38] to find self-similarity, power-law and lognormal marginals patterns in the number of BGP updates that a BGP router receives per time bin, and then used such patterns to detect different types of BGP anomalies. Al-Musawi et al. [39] investigated the deterministic, recurrent and non-linear properties of BGP updates from BGP routers, defined the normality of BGP update volumes, and applied recurrence quantification analysis to detect BGP instability. All these works defined the normality of BGP behavior based only on the volume of BGP updates (albeit in different ways) and tried to use such normality to detect anomalies. I-seismograph however uses *all* key BGP attributes known to reflect BGP dynamics and considers the long-term evolution of BGP in order to offer a more comprehensive and long-standing view of BGP normality. Moreover, I-seismograph can not only detect BGP anomalies, but can also further quantify the deviation of various anomalies from the normality.

A few research projects further studied how to classify BGP anomalies. Research in [40] proposed an Internet routing forensics (IRF) framework that uses supervised machine learning to detect and classify the impact on BGP from Internet-wide intrusions and pathological events. Similarly, the work in [41] introduced a framework to experiment with different machine learning algorithms for training and detection of BGP anomalies. Additionally, the work in [42] proposed a knowledge-based classification to detect and distinguish different BGP anomalies. Dou et al. [43] proposed an unsupervised machine learning via a hierarchical clustering algorithm to detect and classify BGP anomalies. Finally, researchers also studied BGP anomaly classification based on support vector machine models and hidden Markov models [44], as well as the efficacy

of Naïve Bayes and decision tree J48 classifiers [45]. The key difference between these works and I-seismograph is that while these works address the classification of BGP anomalies, I-seismograph focuses on quantifying how far different clusters/classes of anomalous BGP data deviate from the normal state of BGP.

Researchers have also attempted to investigate the origin or root causes of Internet routing behavior. Most analyses focus on specific, individual routing changes (e.g., [46], [47], [48], [49], [50], [51], [52], [53]), while some focus on the root cause of a routing phenomenon that occurs at a large, global scale (e.g., [54], [36], [55]). While it is not the focus of I-seismograph to analyze the origin or root causes of any Internet routing behavior, it can be effective in facilitating the analysis of anomalous routing behavior, in that it can identify abnormal BGP data to more easily capture what happened to BGP during a period in question (see Sec. VI).

Also extensively investigated are the effects on BGP of various events, such as router misconfigurations (e.g., [2], [56], [57]), security attacks([1], [5], [58], [59]), natural disasters (e.g., [60], [61], [62], [20], [19]), electricity outage (e.g., [18]), censorship (e.g., [55], [63]), or large-scale high-impact events that affect many IP prefixes ([64]). These works discovered that under severe conditions the Internet routing could experience a much higher level of dynamics. Although informative, however, these studies are about individual cases and are not meant to provide an approach to systematically observing, detecting, and quantifying the anomalies that BGP may experience.

It is worth noting that even only considering the related studies published after the initial publication of I-seismograph in [65] (these studies are included in the discussions above), I-seismograph still makes unique contributions. Compared to recent studies that mostly relate to measuring BGP dynamics ([29], [31]) or detecting or classifying BGP anomalies ([39], [35], [41], [44], [45]), I-seismograph focuses on deriving the *long-term* normal state of BGP and quantifying to what extent BGP dynamics or various anomalies may deviate from the long-term normal state. I-seismograph also differs from the work in [46], [55], as it does not focus on investigating the origin or root causes of Internet routing behaviors; however, it can effectively facilitate the analysis of anomalous routing behavior as demonstrated in Sec. VI.

IX. Conclusions

While the Internet is a critical infrastructure of our society, little has been done to monitor it as a whole and report the impact—which we also call an Internet earthquake—that it may be experiencing at any time. The fact that the Internet is a large, complex moving target makes this task particularly challenging.

To address this problem, we devised a measurement tool called I-seismograph. It focuses on the most essential function of the Internet—routing, and the *de facto* inter-domain routing protocol—BGP. Considering that BGP is a complex routing protocol concerning IP prefixes from the entire IP address space and involving BGP routers from all over the Internet, plus BGP's constant evolution over many years, I-seismograph uses a two-phase clustering method to discover the normal and abnormal states of the Internet, measures how much the BGP dynamics deviate from normalcy during any time, and reports both the magnitude and the direction of the deviation.

I-seismograph is easy to use, and can measure an Internet earthquake using a heavyweight mode or a lightweight mode, either during an arbitrary period from the past or in real time. We have demonstrated its usage and shown the results from applying I-seismograph during different monitoring periods over the last 16 years. We have also validated it and found it is both accurate and consistent. Finally, by identifying abnormal BGP data and enabling the comparison of abnormal BGP data against the normal data, I-seismograph can help analyze and diagnose what happened to BGP during an Internet earthquake, such as which ASes are affected the most or which AS path segments surged most significantly in BGP updates.

References

[1] Dyn Research, "2031 networks out in India," http://b2b.renesys.com/eventsbulletin/2016/03/IN-1458416970.html, 2016.

[2] A. Toonk, "Massive route leak causes Internet slowdown," http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/, 2015.

[3] D. Reisinger, "Time Warner Cable suffers massive outage nationwide," http://www.cnet.com/news/time-warner-cable-suffers-massive-outage-nationwide/, 2014.

[4] L. Franceschi-Bicchierai, "Internet blackout sweeps Syria, again," http://mashable.com/2014/03/20/syria-goes-almost-completely-offline-again/, 2014.

[5] A. Toonk, "A BGP leak made in Canada," http://www.bgpmon.net/a-bgp-leak-made-in-canada/, 2012.

[6] E. Zmijewski, "Indonesia Hijacks the World," http://research.dyn.com/2014/04/indonesia-hijacks-world/, 2014.

[7] A. Toonk, "Chinese ISP hijacks the internet," http://bgpmon.net/blog/?p=282, April 2010.

[8] J. Li, M. Guidero, Z. Wu, E. Purpus, and T. Ehrenkranz, "BGP routing dynamics revisited," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 37, no. 2, pp. 7–16, April 2007.

[9] RIPE NCC, "RIPE routing information service raw data," http://data.ris.ripe.net/, (date last accessed on 2017-06-01).

[10] Univ. of Oregon, "Route Views Project," http://www.routeviews.org/, (date last accessed on 2017-06-01).

[11] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. Wu, and L. Zhang, "Observation and analysis of BGP behavior under stress," November 2002.

[12] C. Labovitz, G. R. Malan, and F. Jahanian, "Internet routing instability," vol. 6, no. 5, pp. 515–528, 1998.

[13] J. Han and M. Kamber, *Data Mining: Concepts and Techniques, 2/e.* Morgan Kaufmann Publishers, 2006.

[14] A. Lakhina, M. Crovella, and C. Diot, "Mining anomalies using traffic feature distributions," in *ACM SIGCOMM*, 2005, pp. 217–228.

[15] Computer Emergency Response Team, "CERT advisory CA-2001-19 Code Red worm exploiting buffer overflow in IIS indexing service DLL," http://www.cert.org/advisories/CA-2001-19.html, July 2001.

[16] ——, "CERT advisory CA-2001-26 Nimda worm," http://www.cert.org/advisories/CA-2001-26.html, September 2001.

[17] ——, "CERT advisory CA-2003-04 MS-SQL server worm," http://www.cert.org/advisories/CA-2003-04.html, January 2003.

[18] J. Cowie, A. Ogielski, B. Premore, E. Smith, and T. Underwood, "Impact of the 2003 blackouts on Internet communications," http://www.renesys.com/news/2003-11-21/Renesys_BlackoutReport.pdf, November 2003.

[19] A. P. James Cowie and T. Underwood, "Impact of hurricane Katrina on Internet infrastructure," http://research.dyn.com/content/uploads/2013/05/Renesys-Katrina-Report-9sep2005.pdf, 2005.

[20] S. LaPerriere, "Taiwan earthquake fiber cuts: a service provider view," in *NANOG 39*, February 2007.

[21] E. Zmijewski, "Mediterranean cable break," http://www.renesys.com/blog/2008/01/mediterranean-cable-break.shtml, January 2008.

[22] Dyn Research, "Egypt leaves the Internet," https://dyn.com/blog/egypt-leaves-the-internet/, 2011.

[23] A. Toonk, "What caused today's Internet hiccup," http://www.bgpmon.net/what-caused-todays-internet-hiccup/, 2014.

[24] Archana Kesavan, "SEA-ME-WE-4 cable fault has ripple effects across networks," https://blog.thousandeyes.com/smw-4-cable-fault-ripple-effects-across-networks/, 2016.

[25] H. Yan, R. Oliveira, K. Burnett, D. Matthews, L. Zhang, and D. Massey, "BGPmon: A real-time, scalable, extensible monitoring system," in *IEEE Proceedings of Cybersecurity Applications and Technologies Conference for Homeland Security*, 2009, pp. 212–223.

[26] C. Orsini, A. King, D. Giordano, V. Giotsas, and A. Dainotti, "BGPStream: a software framework for live and historical BGP data analysis," in *ACM Proceedings of the Internet Measurement Conference*, 2016, pp. 429–444.

[27] M. Roughan, W. Willinger, O. Maennel, D. Perouli, and R. Bush, "10 lessons from 10 years of measuring and modeling the Internet's autonomous systems," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 9, pp. 1810–1821, 2011.

[28] A. Elmokashfi, A. Kvalbein, and C. Dovrolis, "On the scalability of BGP: the roles of topology growth and update rate-limiting," in *Proceedings of the ACM CoNEXT Conference*, 2008, p. 8.

[29] A. Elmokashfi and A. Dhamdhere, "Revisiting BGP churn growth," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 44, no. 1, pp. 5–12, 2013.

[30] J. Rexford, J. Wang, Z. Xiao, and Y. Zhang, "BGP routing stability of popular destinations," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*. ACM, 2002, pp. 197–202.

[31] S. Papadopoulos, G. Theodoridis, and D. Tzovaras, "BGPfuse: using visual feature fusion for the detection and attribution of BGP anomalies," in *Proceedings of the Tenth ACM Workshop on Visualization for Cyber Security*, 2013, pp. 57–64.

[32] L. Colitti, G. Battista, I. Marinis, F. Mariani, M. Pizzonia, and M. Patrignani, "BGPlay," http://www.ris.ripe.net/bgplay.

[33] L. Colitti, G. Di Battista, F. Mariani, M. Patrignani, and M. Pizzonia, "Visualizing interdomain routing with BGPlay," *Journal of Graph Algorithms Applications*, vol. 9, no. 1, pp. 117–148, 2005.

[34] M. Lad, L. Zhang, and D. Massey, "Link-rank: A graphical tool for capturing BGP routing dynamics," in *IEEE/IFIP Network Operations and Management Symposium (NOMS)*, vol. 1, 2004, pp. 627–640.

[35] B. Al-Musawi, P. Branch, and G. Armitage, "BGP anomaly detection techniques: A survey," *IEEE Communications Surveys Tutorials*, 2016.

[36] S. Deshpande, M. Thottan, T. K. Ho, and B. Sikdar, "An online mechanism for BGP instability detection and analysis," *IEEE Transactions on Computers*, vol. 58, no. 11, pp. 1470–1484, 2009.

[37] B. A. Prakash, N. Valler, D. Andersen, M. Faloutsos, and C. Faloutsos, "BGP-lens: Patterns and anomalies in Internet routing updates," in *Proceedings of the ACM Conference on Knowledge Discovery and Data Mining (SIGKDD)*, 2009, pp. 1315–1324.

[38] P. Abry and D. Veitch, "Wavelet analysis of long-range-dependent traffic," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 2–15, 1998.

[39] B. Al-Musawi, P. Branch, and G. Armitage, "Detecting BGP instability using recurrence quantification analysis (RQA)," in *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*. IEEE, 2015, pp. 1–8.

[40] J. Li, D. Dou, Z. Wu, S. Kim, and V. Agarwal, "An Internet routing forensics framework for discovering rules of abnormal BGP events," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 35, no. 5, pp. 55–66, October 2005.

[41] I. O. de Urbina Cazenave, E. Köşlük, and M. C. Ganiz, "An anomaly detection framework for BGP," in *IEEE International Symposium on Innovations in Intelligent Systems and Applications*, 2011, pp. 107–111.

[42] J. Li, D. Dou, S. Kim, H. Qin, and Y. Wang, "On knowledge-based classification of abnormal BGP events," in *Proceedings of the International Conference on Information Systems Security (ICISS)*, December 2007, pp. 267–271 (short paper).

[43] D. Dou, J. Li, H. Qin, S. Kim, and S. Zhong, "Understanding and utilizing the hierarchy of abnormal BGP events," in *SIAM International Conference on Data Mining (SDM)*, Minneapolis, Minnesota, April 2007, pp. 457–462 (short paper).

[44] N. M. Al-Rousan and L. Trajković, "Machine learning models for classification of BGP anomalies," in *IEEE International Conference on High Performance Switching and Routing*, 2012, pp. 103–108.

[45] M. Ćosović, S. Obradović, and L. Trajković, "Classifying anomalous events in BGP datasets," in *IEEE Canadian Conference on Electrical and Computer Engineering*, 2016, pp. 1–4.

[46] U. Javed, I. Cunha, D. Choffnes, E. Katz-Bassett, T. Anderson, and A. Krishnamurthy, "PoiRoot: Investigating the root cause of interdomain path changes," in *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 43, no. 4, 2013, pp. 183–194.

[47] J. Wu, Z. M. Mao, J. Rexford, and J. Wang, "Finding a needle in a haystack: Pinpointing significant BGP routing changes in an IP network," in *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2005, pp. 1–14.

[48] M. Caesar, L. Subramanian, and R. Katz, "Towards localizing root causes of BGP dynamics," UC Berkeley, Computer Science Division, Tech. Rep. UCB/CSD-04-1302, 2004.

[49] D. Chang, R. Govindan, and J. Heidemann, "The temporal and topological characteristics of BGP path changes," in *Proceedings of the International Conference on Network Protocols*, November 2003, pp. 190–199.

[50] C. Labovitz, G. Malan, and F. Jahanian, "Origins of Internet routing instability," *IEEE INFOCOM '99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No.99CH36320)*, vol. 1, no. c, 1999.

[51] M. Lad, R. Oliveira, B. Zhang, and L. Zhang, "Understanding resiliency of Internet topology against prefix hijack attacks," in *Proceedings of the International Conference on Dependable Systems and Networks*. IEEE Computer Society, 2007, pp. 368–377.

[52] H. Ballani, P. Francis, and X. Zhang, "A study of prefix hijacking and interception in the Internet," in *ACM SIGCOMM*, 2007, pp. 265–276.

[53] K. T. Latt, Y. Ohara, S. Uda, and Y. Shinoda, "Analysis of IP prefix hijacking and traffic interception," *International Journal of Computer Science and Network Security*, vol. 10, no. 7, pp. 22–31, 2010.

[54] A. Feldmann, O. Maennel, Z. Mao, A. Berger, and B. Maggs, "Locating Internet routing instabilities," August 2004.

[55] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescapé, "Analysis of country-wide Internet outages caused by censorship," in *Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC)*, 2011, pp. 1–18.

[56] M. S. Siddiqui, D. Montero, M. Yannuzzi, R. Serral-Gracià, and X. Masip-Bruin, "Route leak identification: A step toward making inter-domain routing more reliable," in *IEEE International Conference on the Design of Reliable Communication Networks (DRCN)*, 2014, pp. 1–8.

[57] R. Mahajan, D. Wetherall, and T. Anderson, "Understanding BGP misconfiguration," in *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 32, no. 4, 2002, pp. 3–16.

[58] R. Lychev, S. Goldberg, and M. Schapira, "Brief announcement: network-destabilizing attacks," in *Proceedings of the ACM Symposium on Principles of Distributed Computing*, 2012, pp. 331–332.

[59] J. Cowie, A. Ogielski, B. Premore, and Y. Yuan, "Internet worms and global routing instabilities," in *Proc. of SPIE International symposium on Convergence of IT and Communication*, July 2002, pp. 195–199.

[60] J. Heidemann, L. Quan, and Y. Pradkin, "A preliminary analysis of network outages during hurricane Sandy," University of Southern California, Information Sciences Institute, Tech. Rep. ISI-TR-685, November 2012.

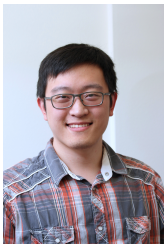
[61] Y. Liu, X. Luo, R. K. Chang, and J. Su, "Characterizing inter-domain rerouting by betweenness centrality after disruptive events," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 6, pp. 1147–1157, 2013.

[62] ——, "Characterizing inter-domain rerouting after Japan earthquake," in *International Conference on Research in Networking*, 2012, pp. 124–135.

[63] Y. Shavitt and N. Zilberman, "Arabian nights: Measuring the Arab Internet during the 2011 events," *IEEE Network*, vol. 26, no. 6, pp. 75–80, 2012.

[64] M. Chen, M. Xu, Q. Li, and Y. Yang, "Measurement of large-scale BGP events: Definition, detection, and analysis," *Computer Networks*, vol. 110, pp. 31–45, 2016.

[65] J. Li and S. Brooks, "I-seismograph: Observing and measuring Internet earthquakes," in *The 30th IEEE International Conference on Computer Communications (INFOCOM)*, Shanghai, China, April 2011, pp. 2624–2632.



Mingwei Zhang is a Ph.D. candidate in the Department of Computer and Information Science, University of Oregon (UO), Eugene, OR, USA, and conducts his research in the Network & Security Research Laboratory at UO. His research interests include Internet routing monitoring, inter-domain routing security, and distributed denial-of-service (DDoS) modeling and defense. He received his B.E. degree in network engineering from Beijing Unviersity of Posts and Telecommunications (BUPT), Beijing, China, in 2012, with an undergraduate thesis in bioinformatics.

Jun Li received the B.S. degree from Peking University in 1992, the M.E. degree from the Chinese Academy of Sciences in 1995 (with a Presidential Scholarship), and the Ph.D. degree (with Outstanding Doctor of Philosophy Hons.) from UCLA in 2002, all in computer science. He is currently a Professor with the University of Oregon, where he also directs the Network and Security Research Laboratory, Department of Computer and Information Science, and serves as the Founding Director of the Center for Cyber Security and Privacy. He has authored a research book on disseminating security updates over the Internet and over 70 peer-reviewed research papers. Currently, he is researching Internet monitoring and forensics, Internet privacy, software-defined networking, social networking, cloud computing, Internet of things, and various network security topics. His research is focused on computer networks, distributed systems, and network security. He has served on U.S. National Science Foundation research panels and 70 international technical program committees, including chairing several of them. He currently serves on the Editorial Board of the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING.

Scott Brooks is a Software Engineer at Google Inc. where he specializes in distributed systems. He received his M.S. degree in computer science from Department of Computer and Information Science, University of Oregon (UO), Eugene, OR, USA, in 2011 and conducted his research in the Network & Security Research Laboratory at UO.

APPENDIX

A. Collectors

The current version of I-seismograph utilizes the publicly available BGP data archive providers, including all the collectors from RouteViews and RIPE. Table I lists all the data collectors we use and their corresponding URLs.

Collector name	URL
RouteViews CHICAGO	ftp.routeviews.org/route-views.chicago/
RouteViews EQIX	ftp.routeviews.org/route-views.eqix/
RouteViews ISC	ftp.routeviews.org/route-views.isc/
RouteViews JINX	ftp.routeviews.org/route-views.jinx/
RouteViews KIXP	ftp.routeviews.org/route-views.kixp/
RouteViews LINX	ftp.routeviews.org/route-views.linx/
RouteViews NWAX	ftp.routeviews.org/route-views.nwax/
RouteViews PERTH	ftp.routeviews.org/route-views.perth/
RouteViews SAOPAULO	ftp.routeviews.org/route-views.saopaulo/
RouteViews SFMIX	ftp.routeviews.org/route-views.sfmix/
RouteViews SG	ftp.routeviews.org/route-views.sg/
RouteViews SOXRS	ftp.routeviews.org/route-views.soxrs/
RouteViews SYDNEY	ftp.routeviews.org/route-views.sydney/
RouteViews TELXATL	ftp.routeviews.org/route-views.telxatl/
RouteViews WIDE	ftp.routeviews.org/route-views.wide/
RouteViews 2	ftp.routeviews.org/
RouteViews 3	ftp.routeviews.org/route-views3/
RouteViews 4	ftp.routeviews.org/route-views4/
RouteViews 6	ftp.routeviews.org/route-views6/
RIPE RRC 00	data.ris.ripe.net/rrc00/
RIPE RRC 01	data.ris.ripe.net/rrc01/
RIPE RRC 02	data.ris.ripe.net/rrc02/
RIPE RRC 03	data.ris.ripe.net/rrc03/
RIPE RRC 04	data.ris.ripe.net/rrc04/
RIPE RRC 05	data.ris.ripe.net/rrc05/
RIPE RRC 06	data.ris.ripe.net/rrc06/
RIPE RRC 07	data.ris.ripe.net/rrc07/
RIPE RRC 08	data.ris.ripe.net/rrc08/
RIPE RRC 09	data.ris.ripe.net/rrc09/
RIPE RRC 10	data.ris.ripe.net/rrc10/
RIPE RRC 11	data.ris.ripe.net/rrc11/
RIPE RRC 12	data.ris.ripe.net/rrc12/
RIPE RRC 13	data.ris.ripe.net/rrc13/
RIPE RRC 14	data.ris.ripe.net/rrc14/
RIPE RRC 15	data.ris.ripe.net/rrc15/
RIPE RRC 16	data.ris.ripe.net/rrc16/
RIPE RRC 18	data.ris.ripe.net/rrc18/
RIPE RRC 19	data.ris.ripe.net/rrc19/
RIPE RRC 20	data.ris.ripe.net/rrc20/
RIPE RRC 21	data.ris.ripe.net/rrc21/

TABLE I: Complete list of all BGP data collectors used in I-seismograph

Note that collector RRC02, RRC08, and RRC09 have stopped updating their data archives and only provide historical data. We use such collectors for the analysis of historical events only.

B. BGP Databin Length Choice

I-seismograph's basic data processing unit is BGP *databin*, which is a summary of BGP activities over a constant time period. Deciding the length of this period is a tradeoff: It cannot be too short; otherwise, the BGP activities within every databin will always be too sparse, and it will be difficult to distinguish normal and abnormal level of activities. It cannot be too long either; otherwise, I-seismograph will suffer from a slow response time since it will take I-seismograph at least the length of one databin to process and report the impact on BGP.

We measured, for different lengths of BGP databin, how many BGP announcements, withdrawals, and updates usually occur. Fig. 1 shows the results. Clearly, one minute would be a reasonable choice.

C. Short-term Clustering Stopping Criterion

When conducting the short-term clustering for a reference period, we need to make sure the final s-normal cluster will contain at least 50% data from the original input, and the databins in the same cluster are much more similar than those from different clusters. There are indeed many different stop criteria for clustering, but in order to meet the requirements above, we found that it works best by checking if the intra-cluster distance is no more than 20% inter-cluster distance, as shown in Fig. 2.

D. Long-term Clustering Stopping Criterion

In the long-term clustering (Section III-E2), if the difference between the intra-distance of a cluster and that of its parent cluster is no more than a threshold, we decide the cluster is not "tighter" than its parent cluster, and we will not further divide the cluster. We experimented with 16 different long-term clustering processes and tested how all the processes may be affected by different threshold values ranging from 0.1% to 99%. As shown in Fig. 3, we found that every process generates basically the same number of clusters when the threshold is 2% or less, but the number decreases when it is more than 2%. Therefore, we choose 1% as a safe threshold value to ensure the long-term clustering obtains the largest number of clusters.

E. Impact Calculation Formula Basis

In calculating the deviation distance along each attribute, say A_i, we found that along each attribute the databins in the normal clusters (i.e., normal databins) are mostly within $[\mu_i-\sigma_i, \mu_i+\sigma_i]$ (as shown in Table II), where μ_i and σ_i are respectively the mean and standard deviation of all the databins from the normal cluster along attribute A_i. So we use the databin's absolute distance from $[\mu_i-\sigma_i, \mu_i+\sigma_i]$ as its deviation along attribute A_i.

	mean±std_dev
WW	100.0
WADup	100.0
Withdraw	92.978
WADiff	90.247
AW	90.557
Announce	92.879
AADiff	96.439
Update	93.034
AADup2	91.950
AADup1	91.950

TABLE II: Percentage of attribute values that fall into mean ± standard deviation.

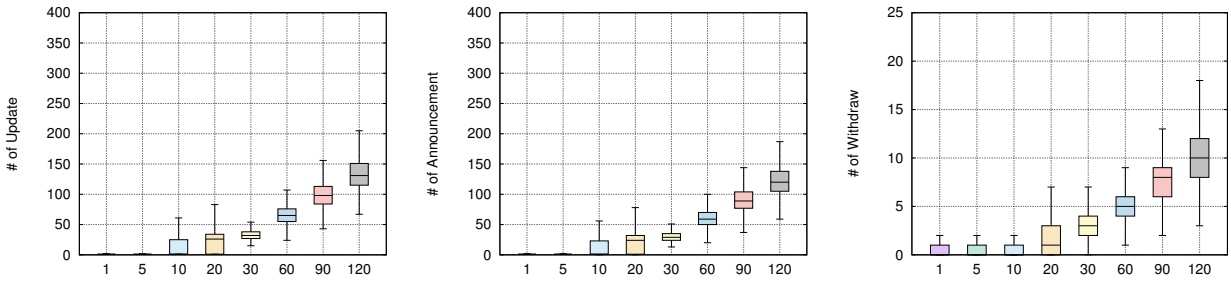


Fig. 1: Boxcharts of the # of three BGP dynamics attributes per databin with different lengths of databins, ranging from 1 second to 120 seconds.

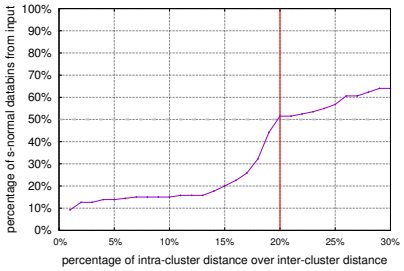


Fig. 2: Short-term clustering effect with different intra- vs. inter-cluster distance percentage.

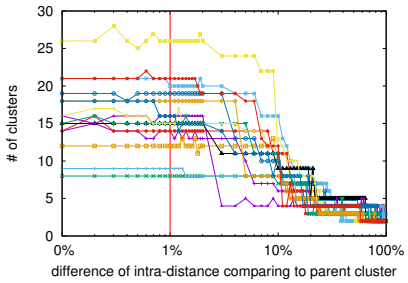


Fig. 3: Long-term clustering effect with different child- vs. parent-cluster intra-distance percentage.

F. Comparison of Short-term Normal Clusters from Different Days and Periods

We conducted an experiment to study how short-normal clusters from different days differ. We selected a four-week reference period for each year from 2008 to 2016, conducted short-term clustering over all these periods, and compared the s-normal clusters from the same reference period as well as short-term clusters from different reference periods. As shown in Fig. 4, clearly, the s-normal clusters are slightly different over different days from the same reference period, but can be more significantly different over different days from different reference periods.

G. Convergency Validation using Only Reference Periods Data

We also used the data from reference periods to test the convergency of I-seismograph. From Fig. 5, we can clearly see that the convergency test results using data only from reference periods are very close to the original results that use both the reference and monitoring periods, as shown in Section IV.B.

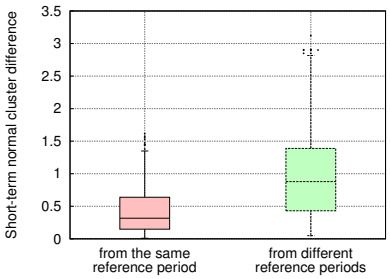


Fig. 4: The differences of short-term normal clusters for different days from either the same reference period or different reference periods.

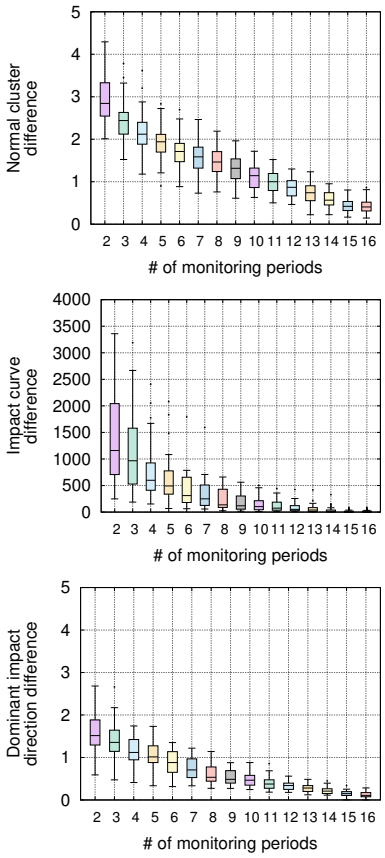


Fig. 5: The convergency of I-seismograph with data only from reference periods.