Analyzing the Internet Stability in Presence of Disasters

Francesco Palmieri, Ugo Fiore, Aniello Castiglione, Fang-Yie Leu, Alfredo De Santis

Analyzing the Internet Stability in Presence of Disasters

Francesco Palmieri[1], Ugo Fiore[2⋆], Aniello Castiglione[3], Fang-Yie Leu[4], and Alfredo De Santis[3]

[1] Dipartimento di Ingegneria Industriale e dell'Informazione
Seconda Università di Napoli
Via Roma 29, Aversa (CE), I-81031, Italy
fpalmier@unina.it

[2] Information Services Center, Università Federico II
Via Cinthia 5, I-80126, Napoli, Italy
ufiore@unina.it

[3] Dipartimento di Informatica, Università di Salerno
Via Ponte don Melillo, I-84084, Fisciano (SA), Italy
castiglione@ieee.org, ads@dia.unisa.it

[4] Department of Computer Science, Tunghai University
No.1727, Sec.4, Taiwan Boulevard, Xitun District, Taichung 40704, Taiwan
leufy@thu.edu.tw

Abstract. The Internet is now a critical infrastructure for the modern, information-based, e-Society. Stability and survivability of the Internet are thus important, especially in presence of catastrophic events which carry heavy societal and financial impacts. In this work, we analyze the stability of the inter-domain routing system during several large-scale catastrophic events that affected the connectivity of massive parts of the address space, with the objective of acquiring information about degradation of service and recovery capabilities.
Results show that the Internet has maintained good responsiveness: service disruption has been contained and recovery times have been fast, even after catastrophic events. However, combining the view provided by the routing table and the view originated by the analysis of the BGP updates is not a trivial task, as such phenomena need to be analyzed at multiple time scales.

Keywords: Internet Resilience, BGP, Disasters, Critical Infrastructures, Catastrophic Events

1 Introduction

Much of the social life is now reliant on interactions carried out remotely, and a significant fraction of these interactions happen over the Internet that assumes

⋆ Corresponding author: Ugo Fiore, Information Services Center, Università Federico II, Via Cinthia 5, Napoli, I-80126, Italy - Phone: +39081676632, Fax: +39081676628, email: ufiore@unina.it

the role of a critical infrastructure for the modern information-based e-Society. This is also true for money-involving applications such as financial transactions, which make heavy use of the Internet infrastructures. Disruption of service on the Internet would carry catastrophic consequences over these activities: therefore, resilience and survivability of the Internet are now extremely important aspects, both at the business level and at the governmental level.

The impact of an Internet outage on essential economic sectors may in fact be devastating for an entire country. Furthermore, to respond to emergencies in an effective and timely manner, availability of accurate information and ability to disseminate it are critical factors that both depend on the correct functioning of a communication infrastructure. The term *survivability* is generally referred to the ability, in the aftermath of a disruptive event, to recover and quickly return to service levels offered before. While the Internet has become a critical infrastructure, there is no comprehensive knowledge about its expected behavior during crises, particularly in terms of its survivability in presence of large-scale disruptions or failures over its fundamental transport infrastructure. Due to the distributed architecture of the Internet, there are many exchange points around the globe, owned by consortia of service providers who share costs and capacity, where a number of transmission links converge in order to connect networks operated by different organizations. In addition, there are critical connections such as undersea links, forming an essential part of the global Internet. These points and links assume the role of critical assets for the overall Internet coverage and operations, since their failure, due to fiber damage or power outages, may wreak havoc on connectivity of significant portions of the Internet. Fiber damages and power outages may be either due to natural phenomena, such as earthquakes, typhoons, and floods, or man-made disasters consequent to war or terrorist actions. Other service disruptions may originate from malware (e.g., worms) devouring all communication resources during the course of their spread throughout the Internet.

In order to achieve a better understanding of the fundamental dynamics governing the Internet behavior, one must study historical data, recorded over the last decade, that describe the state and evolution of network reachability information, and correlate such data with knowledge about the events occurred at the time data were registered. With this in mind, we analyze the stability and behavior of the routing infrastructure, whose fundamental glue is the inter-domain routing system, empowered by the Border Gateway Protocol (BGP), during several large-scale catastrophic events that affected the connectivity of large regions within the Internet, in order to acquire some information about its fundamental service degradation properties and fault recovery capabilities.

In this work we limit our study to catastrophic events originated by physical causes, disregarding any kind of malicious network/traffic activity that can adversely affect the Internet operations on a large scale. We are interested in analyzing the entity of damage to Internet connectivity, its distribution across the globe, and the time needed to recover together with the effects perceived

on global reachability from several observation points scattered throughout the world.

2 Related Work

Several experiences available in literature focus their attention on the analysis of the Internet behavior in presence of large scale infrastructure failures due to both natural or human-driven causes, such as catastrophic events or worm/malware outbreaks. The study presented in [1] carefully analyzed the BGP system dynamics, during a power outage that affected the connectivity of 3,175 networks in a large number of cities in the eastern United States and Canada. The 2006 earthquake in Taiwan has been extensively analyzed from the BGP point of view in [2], largely focusing on an AS-based perspective. Similarly, in [3] a characterization is presented of BGP recovery times under large-scale failure scenarios associated to disasters or man-made events, resulting in substantial recovery times in presence of massive failures. In addition, the work in [4] evaluates the potentiality of BGP-compliant recovery schemes exploiting route diversity in order to recover from large-scale Internet failures. A survey on the security issues related to disasters, with emphasis on maintaining network access, is presented in [5]. From a more theoretical point of view, the contribution presented in [6] studied the stability of the Internet, as a scale free network with respect to crashes, such as random removal of sites, according to a percolation theory-driven approach. The effects of other kind of events, such as large worm outbreaks on Internet stability has been analyzed in [7].

3 Routing, BGP, and Stability

The number of services running on the Internet continually increases, and so does the network size. This continued growth challenges the capability of routing layer to produce a stable, coherent, and reasonably efficient view of the topological structure of all portions of the network. This is an essential condition for continued delivery of packets to their destination addresses.

3.1 BGP

Adjacent Autonomous Systems (ASes) [8] exchange reachability information about destination Internet address blocks, so that routers can reach a consistent topological view of the network. In turn, this allows consistent routing decisions to be taken, without generating undesirable situations such as conflicts or loops. The de-facto standard protocol for inter-domain routing is the Border Gateway Protocol (BGP). A BGP announcement (BGP UPDATE message) concerns a route, and carries a set of attributes. A mandatory attribute is the AS-PATH, indicating the sequence of ASes to be traversed to reach the listed destinations. A BGP-speaking router at an AS, passing an announcement originated at another BGP peer, prepends its own AS number to the AS-PATH. Each AS makes

its own routing decisions based on several factors, including financial considerations or various agreements with other ASes: the chosen route is not necessarily the shortest one, but it is the more *convenient* one. BGP also provides network administrators with means to influence the routing selection process at other places. A comprehensive source of information about BGP and the network prefixes advertised and withdrawn can be found in the CIDR Report [9].

3.2 Routing Instability

Routing instability can be informally defined as the continuous, and sometimes rapid, change of topological information, so that network reachability fluctuates and cannot be controlled by network administrators: routes become unpredictable. While a small percentage of changes can be expected over all the network — due to normal building and maintenance operations as well as failures — instability may be localized or distributed. When a single router repeatedly withdraws some routes and re-announces them soon after, instability is localized and is then called *route flapping*. Here, we are considering distributed instability, measured at global or at least regional scale. To measure Internet instability, BGP routing statistics provide important data to work with. BGP statistics describe two aspects: the (global) routing table, i.e., the list of all reachable prefixes, and the number, and rates of change, of the routing information updates, i.e., prefix announcements and withdrawals in BGP UPDATE messages. Each of these aspects, if studied in isolation, offers useful information to quantify instability. Analyzing both aspects in combination can provide additional insights.

- The *size of the global routing table* gives an overall measure of the reachability in terms of network prefixes that are announced. Keeping in mind that aggregated prefixes will still be announced even if more specific ones are no longer reachable, reachability of specific prefixes is a more reliable indicator of instability than it is reachability of aggregated prefixes.
- The *number of BGP updates* sent out and received per time unit is a fundamental metric in observing the dynamics of BGP, also provideing an indication of whether BGP peers need to exchange fresh information or not, perhaps as a result of changes in reachability of their connected networks or of communication problems between the routers themselves. Sudden increases in the number of BGP updates per time unit indicate an increased signaling activity and this, in turn, suggest that something is happening which is worth investigating. BGP update message may bring two different kinds of routing information: *prefix announcements* and *withdrawals*. An announcement is a network reachability message, specifying the presence of a new network (identified by its own prefix) that becomes reachable through a specific route. Each time an available route/path for a particular network changes, eventually also due to traffic engineering/management activities, a new announcement is issued from the node ensuring the reachability for

that network and propagated through BGP so far. On the other hand, withdrawals happen when a given path for reaching a particular prefix is no longer preferred or available. When a route fails, in absence of other paths, the BGP peer notifies other peers that the path is no longer valid. Although backup systems or redundant routes/paths are commonly used within the Internet, we expect that a severe outage will have caused some networks to become unreachable due to the sustained nature of the outage, extending beyond backup capabilities or redundancies. BGP sessions that involve networks affected by the outage can thus be broken. When BGP routers peering with BGP routers from affected networks send out explicit withdrawals to notify other BGP routers, it will result in many withdrawal updates. The number of networks affected during the blackout directly affects the number of withdrawal updates.

– The *average AS-PATH length* over the whole Internet is another interesting metric that can be useful to depict the degree of interconnection at the global level. Due to the basic BGP route selection criterion based on preferring the "shortest AS path", when BGP determines the path connecting two different ASes it will select the one going through the least number of hops. Hence as the degree of interconnection between ASes grows, the average AS path tends to become shorter.

While the first two metrics (routing table size and updates count) are related, they do not necessarily agree. Misalignment may result from the superposition of the effects of different events happening simultaneously or from the different frequency of data collection.

4 Analyzing the Internet Stability Dynamics

The simplest way of understanding the fundamental dynamics characterizing the Internet routing system during critical situations, comes from the careful observation of BGP activities, by spotting its resilience and capacity of reacting to adverse conditions. In this study, BGP data collected by the Routing Information Service (RIS) project[5] from RIPE NCC have been used. The aim of RIS is providing Internet operators information about the global routing system current state and its evolution. Routing information is gathered by means of monitoring points. The RIPE RIS project maintains seventeen monitoring points (Remote Route Collectors) in major exchange points across the world. Ten monitoring points are in Europe, four in the US, one in Brazil, one in Japan, and one in Russia. Each monitoring point is basically a BGP-speaking router that makes no announcement of its own but listens to (and records) announcements from its peers. Both BGP updates and routing table dumps are collected and stored. Recall that routing decisions stem from the combination of several factors, which are dependent of the geographical location, the ASes involved, their relationships

[5] https://labs.ripe.net/datarepository/data-sets/routing-information-service-ris-raw-data-set

with other ASes and Tier-1 providers, and financial agreements. Thus, having more than one monitoring point means being able to observe a multifaceted phenomenon (the routing system) from different perspectives and situations. Analysis of routing information collected at each BGP monitoring point can provide a great deal of information about the view that organizations at the collection point have of the Internet. By studying how this information evolves over time, insights can be obtained on the dynamics of path change, spotting trends, cyclic behavior, and periods of instability. In particular, we are interested in detecting, in correspondence of well-documented catastrophic events, compatibly long periods of growth and decay in the routing table dimensions and prefix announcement/withdrawal rates across multiple observation points, indicating a significant and widespread degradation in the overall connectivity and functional behavior of large sections of the Internet.

The advantage of having the monitoring point at a peering point is that the views of all the participants to peering may be observed and combined together. In particular, routing instabilities, even of considerable extent, that are localized to a single AS can be isolated from global failures that affect large portions of the Internet. The updates are collected with an interval of 5 minutes. The routing tables are instantaneous snapshots of the routing tables saved every 8 hours. The amount of data collected in a single monitoring point ranges from about 30 MByte/day for the updates to about 30-60 MByte/day for the routing tables.

It is useful to have a unified view of both the routing tables and the updates with the same sampling interval. Updates have thus been aggregated over the same interval of the routing tables, i.e., 8 hours. A side effect of this aggregation is that the effects of transient phenomena tend to be diluted, since these phenomena are unlikely to span 8 hours or a significant fraction of that time. Occasional router malfunctions, data losses, link saturation, or router reloads affecting either the BGP speakers or the monitoring point, may in fact produce sudden apparent increases or decreases in the number of updates, thus raising false signals of instability that are unrelated to the disruptive effects of the events under observation. The smoothing effect of aggregation will reduce the influence of short-lived glitches, privileging large-scale changes. In addition, observing on a larger time scale will also reduce the effects of time synchronization issues. Unfortunately, in global-scale BGP analysis the observations are aggregated over all networks, and when the amount of BGP updates associated to the event of interest is only a very limited part of the whole baseline update activity propagating throughout the Internet, the statistical variations in the overall update rate introduced by the event of interest may be difficult to appreciate. In this case, in order to pinpoint the specific update activities related to the prefixes really affected from the event, refocusing out attention by restricting the analysis only on the prefixes of interest, to observe the BGP behavior at the individual prefix level becomes of fundamental importance. This can be accomplished by geographically referencing the update data and observing them on a contextualized scale. That is, the updates have been mapped, depending on their prefixes, on a worldwide map to allow an observation of the involved phenomena based

on geographical localization criteria. In order to refine our observations, we analyzed the BGP activity data collected before, during, and after the events of interest, so that the observations before the event can be used as a baseline of the assumed normal behavior. That is, routing tables and updates were collected for analysis over a time window starting three days before the day the critical event occurred and ending three days after. This allows an enough long time to observe the smoothing recovery. Since data have been collected also before critical events, by averaging over three days, it is possible to obtain a more smoothed baseline depicting the state of the network immediately before the event, to be compared with the one visible after the event. So the extent to which the situation returned to normality and the speed of this process can be evaluated. For each event, thus, 21 snapshots of the routing table (i.e., 7 days) and 2016 files containing updates have been analyzed.

4.1 The Events of Interest

The catastrophic events analyzed are different in nature, amplitude of the affected region, duration, and presence/absence of alternate routes. For example, a long-lasting blackout determines the outage of large areas and their address blocks, while a cable failure only involves the connected endpoints and the mutual reachability of networks that were using that connection, provided that no other path existed between them. The events analyzed are reported in Table 1.

Table 1. The considered events.

Type	Location	Date
Earthquake	Taiwan	27 Dec 2006
Earthquake	Japan	11 Mar 2011
Blackout	USA	08 Sep 2011

The significance of discussing two events of the same type (earthquakes) is that in one case the effects were more limited, because there were alternative routes available for many networks. Availability of Internet connection had indeed been, in that circumstance, an important factor for speeding up and coordinating rescue efforts to aid people who were affected in the disaster.

5 Results and Discussion

5.1 Earthquake in Taiwan

An earthquake off the southern coast of Taiwan, approximately 22.8 km southwest of Hengchun, struck on December 26, 2006 at 12:25 UTC (20:25 local time). The earthquake, of magnitude 7.1 on the Richter scale, damaged undersea cables, catastrophically disrupting communications across east Asia, affecting, in

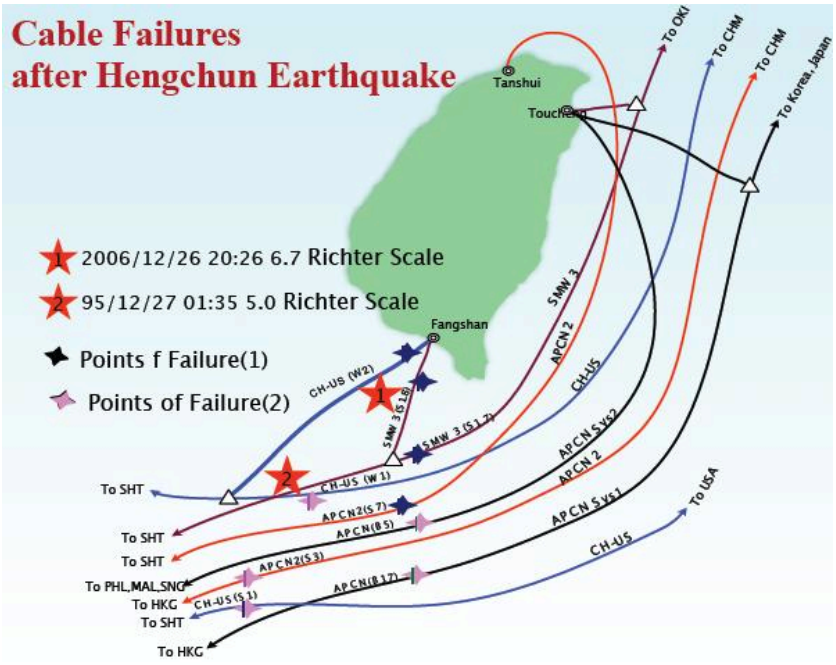
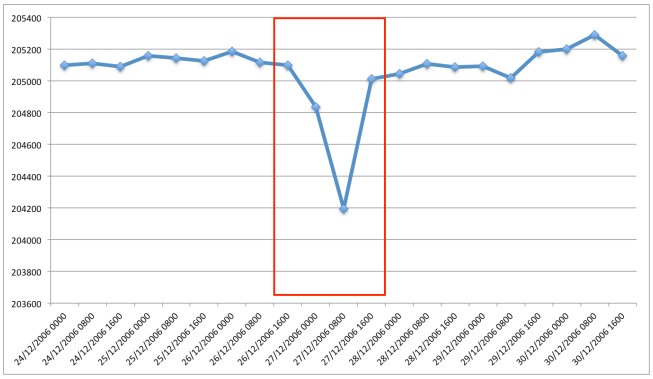


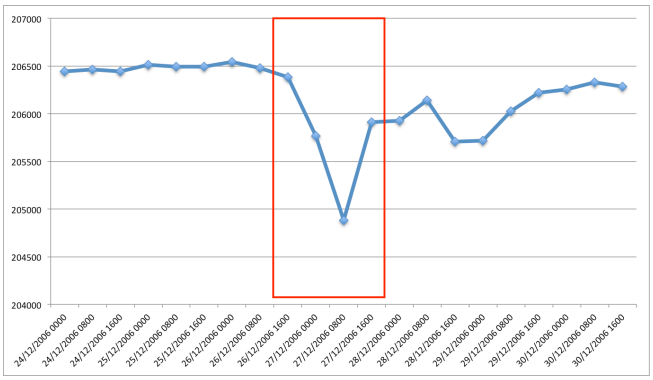
Fig. 1. Earthquake in Taiwan: Affected undersea cables [10]

addition to Taiwan, also Malaysia, Singapore, Thailand and Hong Kong. Telephone and Internet problems were reported in Taiwan, South Korea, China and Japan. Eight submarine cables (see Fig. 1) were severed after the earthquake and its aftershocks, all of which were above magnitude 5 of the Richter scale. Some of the submarine networks affected had backup paths that helped limit the extent of damage. The diversion of all traffic over the backup links caused congestion on these links, with a perceptible slowdown of communications. Links to Europe, in particular the FLAG Europe Asia link, had no such backup available. Communications over that links were thus interrupted and a significant part of Asia near Taiwan and China went back into the pre-Internet era. The effects of these phenomena have been immediately observed on the whole Internet in terms of both BGP update activity and reduction of the available number of prefixes in the routing table (see Figures. 2 and 3). After all the strong aftershocks, the number of routes plummeted by about 800 in NY (Fig. 2(a)) and 1500 in Moscow (Fig. 2(b)).

Fig. 4 displays the number of IP addresses that became unreachable and at their geographical location. A yellow tint on a country indicates the loss of a small number of IP addresses originating from that country; orange means a moderate loss, and red a significant loss. The number of IP addresses shown in Fig. 4 are measured from a monitoring point in Europe.



(a) RRC11 - New York

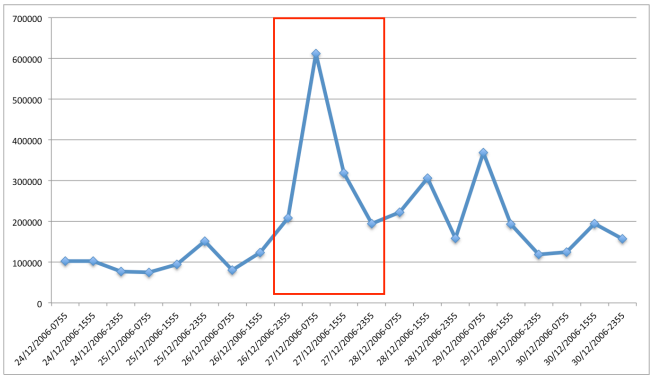


(b) RRC13 - Moscow

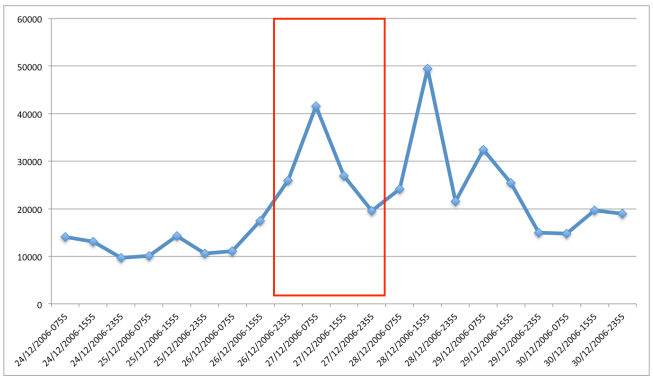
Fig. 2. Earthquake in Taiwan: Routing Table Sizes from NY (a) and Moscow (b) collectors

Looking in detail at Fig. 4, one may observe how a noticeable number of IP addresses from India became unreachable from Europe, as well as some from other countries along the FLAG Europe Asia cable. A large number of IP addresses lost came from the US. This can be explained because the coloring reflects the absolute, not the relative entity of loss. This, combined with the higher number of addresses originating from the US as compared with other countries, suggests that the US can be expected to exhibit a intense shade in the graphs.

Finally, we remark that, interestingly, the average AS-PATH length has stayed steadily at the value 5 across all the analyzed time span. Looking at data more closely, the average AS-PATH length had been equal to 4 (instead of 5) for two 8-hour intervals (24/12/2006-2355 and 25/12/2006-0755), but these intervals preceded the earthquake. In conclusion, the global degree of network interconnection, as seen at the monitoring point, has undergone no significant variation.



(a) Route Announcements



(b) Route Withdrawals

Fig. 3. Earthquake in Taiwan: updates from NY collector: Announcements (a) and Withdrawals (b)

5.2 Earthquake in Japan

On March 11, 2011, a tsunami, unleashed by one of the strongest earthquakes ever measured (magnitude 9.0), devastated the eastern coast of Honshu island, in Japan. Waves as high as 11 meters slammed the coastline and surged inland for several kilometers before retreating back to the sea carrying huge amounts of debris. The wave raced forward at speeds up to 800 km/h and was felt on the other side of the Pacific Ocean.

Casualties and property damage were, unfortunately, dramatic. However, from BGP data one may see that most of the local and transit connections to the Internet stayed stable. In particular, observing the routing table size from most of the collectors no significant falls in the number of routes can be observed in correspondence with the heart quake (see the Amsterdam collector data in Fig. 5(b) as an example). In this case, Internet availability might well have been a factor that facilitated rescue operations. The seas around Japan are a major hub

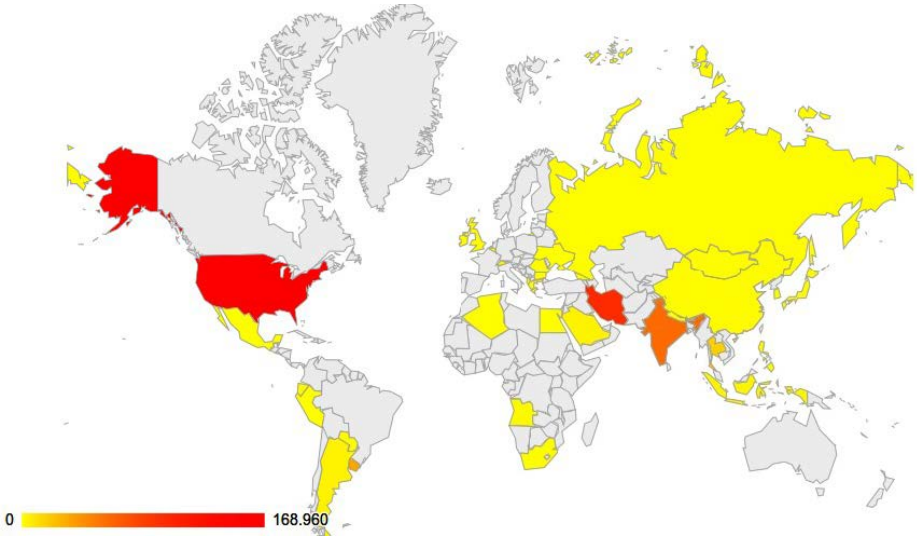
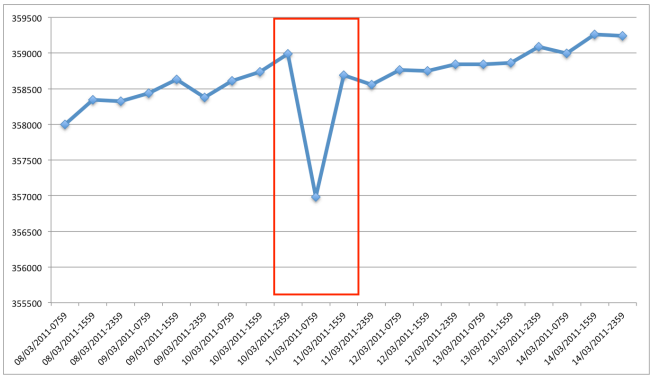


Fig. 4. Earthquake in Taiwan: IP addresses unreachable from the monitoring point

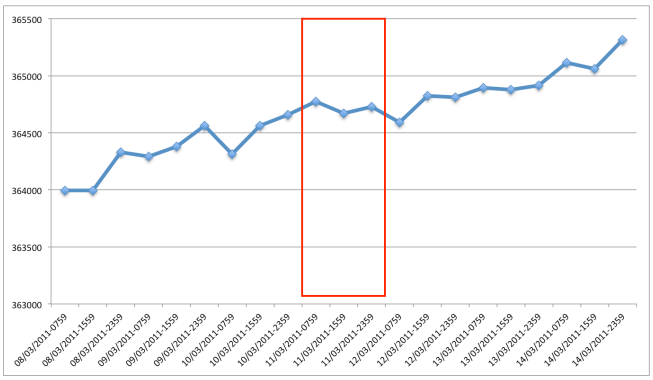
for undersea telecom cables, and a lot of redundant paths are available for the connections attaining to such area. While some undersea cables were damaged, other links stayed active. Though overloaded, those links provided Internet connectivity between the strained Japan and the rest of the world. However, 1969 distinct routes were withdrawn soon after the event, but within the next 8 hours they became available again, and this effect has only been appreciable on the NY collector (Fig. 5(a)).

While our analysis shows that in some places of the world route reachability metrics were not affected in a perceivable way during the event, a significant BGP update activity, in particular in terms of BGP announcements, mainly due to network engineering/rerouting operations has been observed (see Fig. 6). The number of announcements (Fig. 6(a)) grows much more than the number of withdrawals (Fig. 6(b)). There are two reasons for that. The first reason is that the only cancellations that give raise to withdrawals are those where no alternate path is available, whereas in the other case the backup path is simply advertised for the original prefix, thus substituting the previous route. The other reason is that network engineering activities aimed at restoring connectivity, started soon after the disaster had been detected and spanning the following hours, may have created new paths by temporarily relaxing policy-based constraints. This behavior is similar to the other monitoring points. Graphs displaying withdrawals have been omitted to save space.

By analyzing Figure 7(a), one can see that the number of IP addresses that became unreachable was massive. Japan was heavily struck, with 13,4 million IP addresses through 72 routes unreachable from the monitoring point. Note, however, that the monitoring point for Fig. 7(a) is located in in the US, while



(a) RRC11 - New York



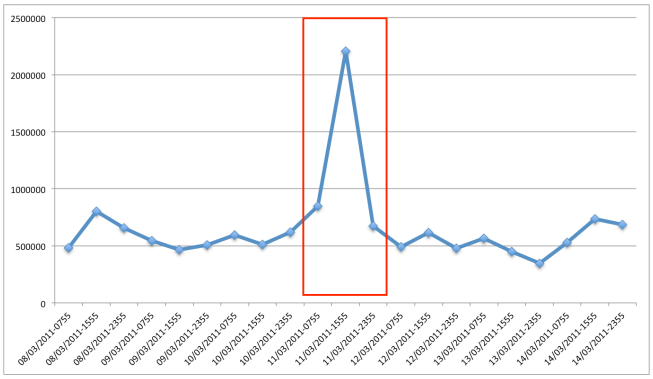
(b) RRC00 - Amsterdam

Fig. 5. Earthquake in Japan: Routing Table Sizes from NY (a) and Amsterdam (b) collectors

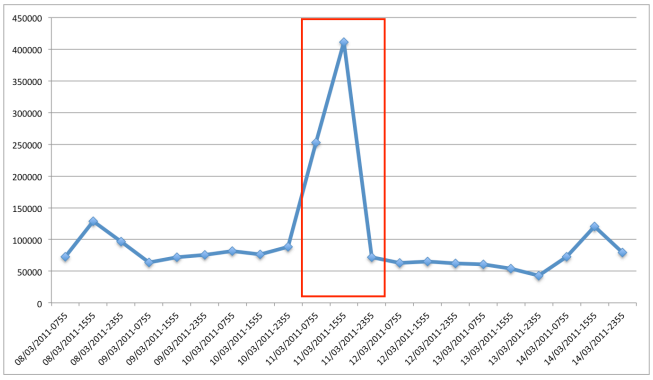
the one for Fig. 4 is in Europe. Therefore the absolute values are not directly comparable. As confirmation of the hypothesis that the climb in the number of routes immediately following the disaster was due to traffic engineering activities, Fig. 7(b) depicts the number of IP addresses reachable through freshly announced routes in the 8 hours following the tsunami. The green shade indicates a large number of IP addresses recovered for a single country. As one can see, Fig. 7(a) and Fig. 7(b) are fairly complementary. The noticeable difference is in a fraction of Japanese addresses that stayed unreachable during the 8 hours immediately after the catastrophe, probably due to the structural damages provoked by the tsunami.

5.3 Blackout in the US

The last event that has been selected for the analysis is the blackout that hit Southern California, USA, on September 8, 2011. The reason why the blackout

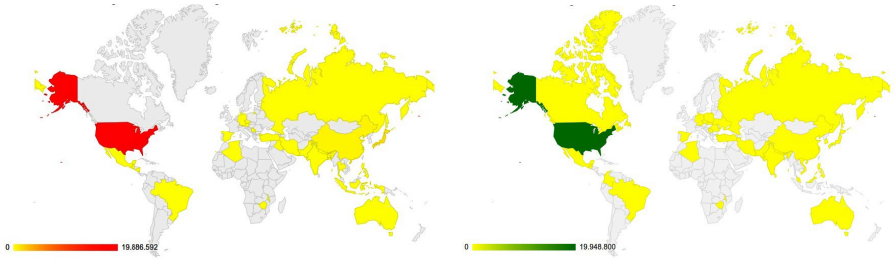


(a) Route Announcements



(b) Route Withdrawals

Fig. 6. Earthquake in Japan: updates from NY collector: Announcements (a) and Withdrawals (b)

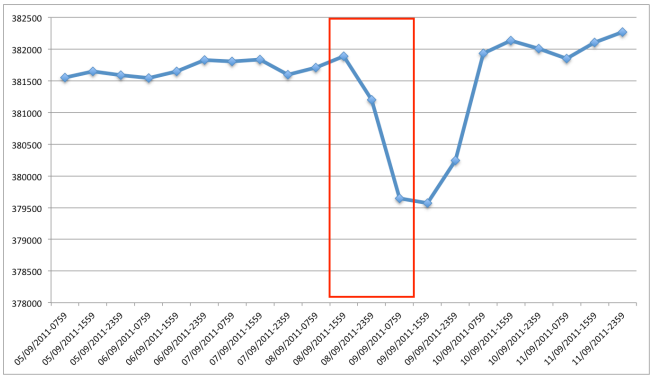


(a) Unreachable addresses (b) Announced addresses

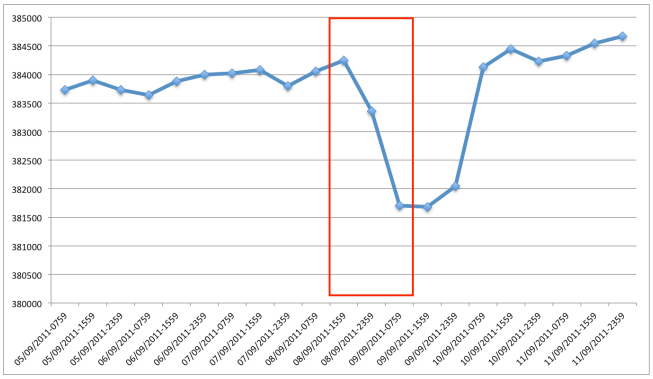
Fig. 7. Earthquake in Japan: IP addresses unreachable (a) and announced (b) at/from the monitoring point

was chosen is that it represents an event of different nature. It is thus interesting to study its effects and the similarities and differences with respect to the

earthquakes discussed above. The massive power outage left more than 8 million citizens without power, also disabling the telephone system, and most wireless phone service, putting people at a severe informational disadvantage [11]. San Diego Gas & Electric claimed that the replacement of faulty equipment at a power substation in Arizona triggered a chain of events that eventually shut down Southwest Powerlink, one of the two major transmission links that connect the San Diego area to the electrical grid for the western United States.



(a) RRC11 - New York

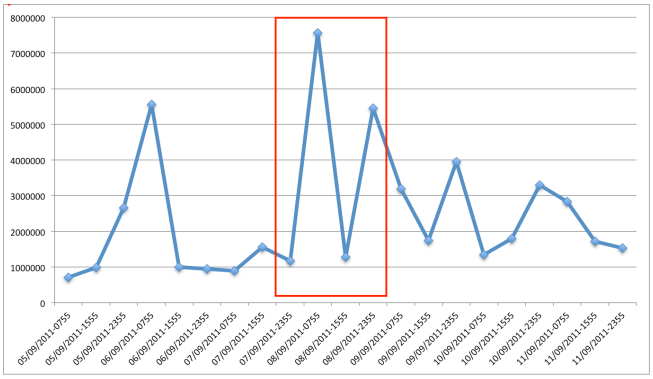


(b) RRC13 - Moscow

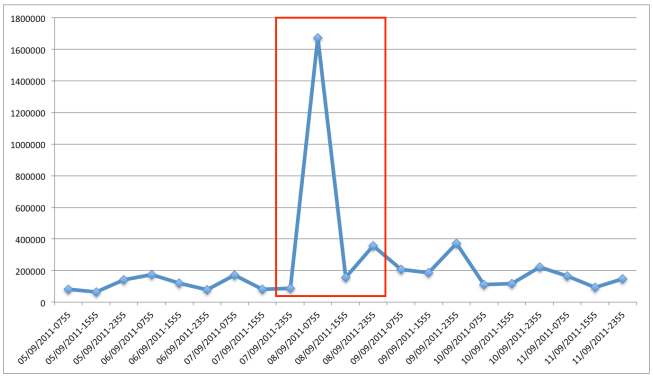
Fig. 8. Blackout in the US: Routing Table Sizes from NY (a) and Moscow (b) collectors

Looking at Fig. 8, a plunge of about 2000 routes is evident. In addition, the loss is gradual, especially as compared with the sudden declines visible in Figures 2 and 5. Possibly, this behavior is due to portions of the network turning unreachable only after the exhaustion of backup power systems, therefore not immediately after the outage but some hours later. As it has been said earlier, analysis of the updates shows, remarkably, substantially similar results for all the events under consideration. From Fig. 9, it is clearly evident that at the

time of the event, the number of withdrawals undergoes a sharp increase, which is unsurprising. However, another peak preceded the event and some oscillatory behavior is visible after it. This suggests that other failures, possibly originated elsewhere in the world, were present at the same time.



(a) Route Announcements



(b) Route Withdrawals

Fig. 9. Blackout in the US - updates from Moscow collector: Announcements (a) and Withdrawals (b)

Also in this case, the average AS-PATH length has not been affected at all by the event, indicating the absence of global degradation in the Internet connectivity within the interested area.

6 Conclusions and Future Work

An analysis of Internet routing statistics when disasters occur, and immediately after, has been performed in this work. Catastrophic events have been selected for

study because they are well documented, and usually there is a wealth of information related to their effects. After gathering BGP statistics and preprocessing data, the number of routes and geo-localization of IP addresses that have become unreachable have been studied. Data show how catastrophic events impact on the reachability of network prefixes, the extent of damages to the Internet global connectivity, the geographical location of the most heavily struck addresses, and the time needed to recover.

Directions for future research include investigation on the degree of correlation, for the same event, between measurements taken at different monitoring points. Moreover, an evaluation of the behavior of BGP updates observed at several time scales would provide interesting insights about the dynamics of the update process.

Acknowledgements

The authors gratefully acknowledge Mr. G. Lanciato for his precious support in data collection.

References

1. Li, J., Wu, Z., Purpus, E.: Toward understanding the behavior of BGP during large-scale power outages. In: Proceedings of IEEE GLOBECOM. (2006)
2. Popescu, A., Underwood, T., Zmijewski, E.: Quaking tables: The Taiwan earthquakes and the Internet routing table. In: APRICOT, Bali. (2007)
3. Sahoo, A., Kant, K., Mohapatra, P.: Characterization of BGP recovery time under large-scale failures. In: Communications, 2006. ICC'06. IEEE International Conference on. Volume 2., IEEE (2006) 949–954
4. Hu, C., Chen, K., Chen, Y., Liu, B.: Evaluating potential routing diversity for internet failure recovery. In: INFOCOM, 2010 Proceedings IEEE, IEEE (2010) 1–5
5. Kiyomoto, S., Fukushima, K., Miyake, Y.: Security issues on IT systems during disasters: a survey. Journal of Ambient Intelligence and Humanized Computing (2013) 1–13
6. Cohen, R., Erez, K., Ben-Avraham, D., Havlin, S.: Resilience of the internet to random breakdowns. Physical review letters **85**(21) (2000) 4626–4628
7. Palmieri, F.: Inter-domain Routing Stability Dynamics During Infrastructure Stress Events: The Internet Worm Menace. I. J. Network Security **6**(1) (2008) 6–14
8. Hawkinson, J., Bates, T.: RFC1930: Guidelines for creation, selection, and registration of an autonomous system (AS). http://tools.ietf.org/html/rfc1930 (March 1996)
9. Bates, T., Smith, P., Huston, G.: CIDR report. http://www.cidr-report.org/as2.0/
10. Winston: Submarine Cables Cut after Taiwan Earthquake in Dec 2006. http://submarinenetworks.com/news/cables-cut-after-taiwan-earthquake-2006
11. Cerf, V.: Natural Disasters and Electric Infrastructure. Internet Computing, IEEE **15**(6) (2011) 103–103