Assessing Resilience of Inter-Domain Routing System under Regional Failures

Yujing Liu[1], Wei Peng[1,2], Jinshu Su[1,2], and Zhilin Wang[3]
[1] College of Computer, National University of Defense Technology
Changsha, China
[e-mail: liuyujing@nudt.edu.cn]
[2] Science and Technology on Parallel and Distributed Processing Laboratory, National University of Defense Technology
Changsha, China
[e-mail: wpeng@nudt.edu.cn]
[3] Education Department, National University of Defense Technology
Changsha, China
[e-mail: wangzhilin@nudt.edu.cn]
*Corresponding author: Yujing Liu

Received July 12, 2014; revised October 2, 2015; revised December 16, 2015; accepted February 8, 2016; published April 30, 2016

Abstract

Inter-domain routing is the most critical function of the Internet. The routing system is a logical network relying on the physical infrastructure with geographical characteristics. Nature disasters or disruptive accidents such as earthquakes, cable cuts and power outages could cause regional failures which fail down geographically co-located network nodes and links, therefore, affect the resilience of inter-domain routing system. This paper presents a model for regional failures in inter-domain routing system called REFER for the first time. Based on REFER, the resilience of the inter-domain routing system could be evaluated on a finer level of the Internet, considering different routing policies of intra-domain and inter-domain routing systems. Under this model, we perform simulations on an empirical topology of the Internet with geographical characteristics to simulate a regional failure locating at a city with important IXP (Internet eXchange Point). Results indicate that the Internet is robust under a city-level regional failure. The reachability is almost the same after the failure, and the reroutings occur at the edge of the Internet, hardly affecting the core of inter-domain routing system.

Keywords: the Internet, inter-domain routing, resilience, regional failure

This research is supported by Program for Changjiang Scholars and Innovative Research Team in University (No.IRT1012); the National Natural Science Foundation of China (Grant Nos. 61303264, 61271252, 61472437, 61202482, 61202486); and the research project of National University of Defense Technology.

http://dx.doi.org/10.3837/tiis.2016.04.009 **ISSN : 1976-7277**

1. Introduction

The Internet is composed of tens of thousands of Autonomous Systems (ASes) defining the administrative authority and the routing policies of different organizations. Routers within each AS run Interior Gateway Protocols (IGPs) such as RIP, OSPF and IS-IS to construct an intra-domain routing system. ASes interconnect with each other via Exterior Gateway Protocol (EGP) to form the inter-domain routing system of the Internet. Nowadays, the de-facto EGP in the Internet is the Border Gateway Protocol (BGP). From the broader perspective, it's very important to study the resilience of the inter-domain routing system under different failures for achieving stable communications in the Internet globally.

The inter-domain routing system is a logical network which greatly relies on the physical infrastructure of interconnected routers. Meanwhile, the distribution of routers exhibits apparent geographical characteristics due to practical deployment. However, the relationships among the logical, physical and geographical networks are fully complicated. For example, a large AS providing service to global customers usually has a massive number of routers located dispersedly in different countries, even different continents; whereas a single area of IXP would host an aggregation of routers belonging to different ASes. Given the dependence of logical and physical topology of the Internet, regional failures may degrade the resilience of inter-domain routing system. Moreover, the local impact may propagate via the logical network globally. More precisely, nature disasters or disruptive accidents such as earthquakes, cable cuts, power outages, and even intentional attacks could cause regional failures which fail down geographically co-located network nodes and links, therefore, affect the resilience of inter-domain routing system. These failed routers and links may belong to different ASes. Therefore, they could affect connections in multiple intra-domain systems, and then affect connections in the inter-domain routing system of the Internet. For example, the Taiwan earthquake in December 2006 broke several undersea cable systems in Asia, leading to hours of communication outages between many Asia sites and U.S. sites [1]. Critical locations should be protected carefully for prevention. It is important to support geographically diverse backup paths for switching after regional failures occur. Our work in this paper will offer valuable method and information that where should be protected and whether the rerouting works to enhance the resilience of the network.

Previous research about assessing resilience of networks has some drawbacks [1-7]. First of all, they are solely based on either logical topology or physical topology. However, the inter-domain routing system is a logical network, while regional failures show distinct geographical characteristics. It is still an open issue to systematically examine how the regional failures affect the logical network. Secondly, according to economic considerations, ASes employ different routing policies to control propagation of routing messages among them. Therefore, it's more realistic to differentiate the routing processes within an AS and among ASes, and apply policy-compliant algorithm in inter-domain routing system instead of simply using shortest path algorithm proposed by previous research. Thirdly, according to assumptions in some related works, a network failure could break down an entire AS. It's not suitable for studies under regional failures. Because an AS usually covers geographically diversified locations so that a geographical fault could just affect parts of its components and lead to degradation of transit capability of an AS.

In this paper, we propose a model for REgional FailurEs in inter-domain Routing system, REFER for short. According to REFER, the inter-domain routing system is modeled by its logical topology annotated with physical and geographical property, and applied two-layer routing algorithm to simulate the shortest path routing process in intra-domain routing system and policy-compliant routing process in inter-domain routing system. To measure the effect of regional failure on an AS in finer granularity, we present the *degradation of transit capability* of AS which is a set of two- and triple-tuples of ASes that aren't able to transmit traffic after regional failures. Furthermore, we characterize the resilience of inter-domain routing system by *change of reachability* and *number of rerouting messages* received by every AS in the Internet. Since the most critical ability of routing system is making routing decisions, reachability can evaluate how the incomplete topology affect the capability; and number of rerouting messages can evaluate the effect of instability of the routing system, because a surge of rerouting messages may exceed the computational capacity of affected routers, and cause a degradation of such capability. Finally, we simulate a regional failure scenario in which all routers in the highest connected city break down. Then the resilience of inter-domain routing system under this regional failure is assessed based on REFER. Valuable insights revealed from the results benefit the improvement of inter-domain routing resilience under regional failures. REFER is a simulation model to assess the resilience of routing system. The regional failures are hypothetical scenarios; moreover, reroutings are performed based on simulations. This model is not for preventing, detecting or reacting to regional failures. It is a useful tool to evaluate how the current Internet performs after this type of failures and whether the enhancement works for future Internet design.

In Section 2, we review the previous work on assessing resilience of routing system of the Internet. We propose our model for regional failures in inter-domain routing system – REFER in Section 3. Then in Section 4, we perform simulations to analyze the routing dynamics described by REFER under the regional failure where all routers locating at an important IXP are taken down. We finally conclude the paper and present future work in Section 5.

2. Related Work

On the one hand, previous efforts on studying the effect of geographical failures on the inter-domain routing system basically focus on particular events. For example, Renesys analyzed the reroutings of the Internet after the Taiwan earthquake in 2006, which were monitored by their own route-collecting system. They found that the local events can have broad impact, and physical failures can be difficult to remedy. Asia is particularly vulnerable [1]. After the Japan earthquake in 2011, Renesys found that the Internet connectivity had survived this event better than anyone would have expected, because Japan created a dense web of domestic and international connectivity in the Internet. The network routed around catastrophic damage and kept the packets flowing, despite terrible chaos and uncertainty [2]. Antony et al. studied the impact of Mediterranean fiber cable cut in 2008 on the Internet, by analyzing the routing data collected by the Routing Information Service of RIPE NCC. Their analysis provided insights that immediately following cable cut, the affecting networks became unreachable. Sites that had arranged for multiple transit providers observed massive reroutings, moving to lower bandwidth or longer distance cable system, which significantly impacted end users and caused instability in routing system [3].

On the other hand, instead of utilizing limited routing data, some research works build models for assessing resilience of networks under regional failures. Neumayer et al. modeled the physical network as a bipartite graph and considered the set of all vertical line segment cuts. Furthermore, they developed a polynomial time algorithm for finding a worst possible cut that would have the maximum effect on network capacity [4]. Motter et al. proposed a cascade-based model for assessing the resilience of complex networks. They demonstrated that networks with a highly heterogeneous distribution of loads, such as the Internet and power grids, were particularly vulnerable to attacks in that a large-scale cascade may be triggered by disabling a single key node [5]. Wu et al. systematically analyzed how the current Internet routing system reacts to various types of failures by developing a realistic failure model, and then pinpointed reliability bottlenecks of the Internet [6]. These models all assume that the topology of routing system of the Internet is either logical or physical. For example, the study of reference [6] assumes that the regional failure will lead to logical AS-level disruptions. However, the reality is much more complicated than these models. The inter-domain routing system is a logical network relying on the physical infrastructure with geographical characteristics. Previous research doesn't consider the dependence of logical and physical topology of the Internet. In our work of this paper, the resilience of the inter-domain routing system is evaluated on a finer level of the Internet, considering how the physical failures affect the router-level intra-domain routing, and then how the router-level failures affect AS-level inter-domain routing systems.

3. Model for Regional Failures in Inter-Domain Routing System

Fig. 1 shows the architecture of our model. It consists of three components: topology mapping, intra-domain routing and inter-domain routing. Every component has the input data representing as an oval; the processing method representing as a diamond; and the output result representing as a rectangle. These three components interact with each other, sharing input or output data. Next we will introduce them in detail and demonstrate their working processes with a simple example as shown in **Fig. 2**.

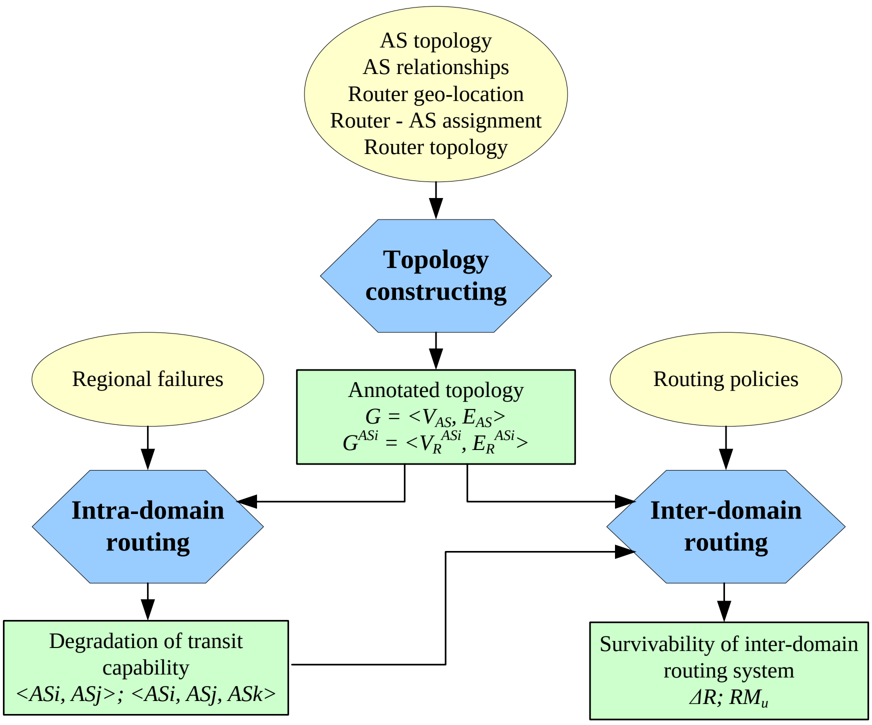

Fig. 1. The architecture of model for regional failures in inter-domain routing system

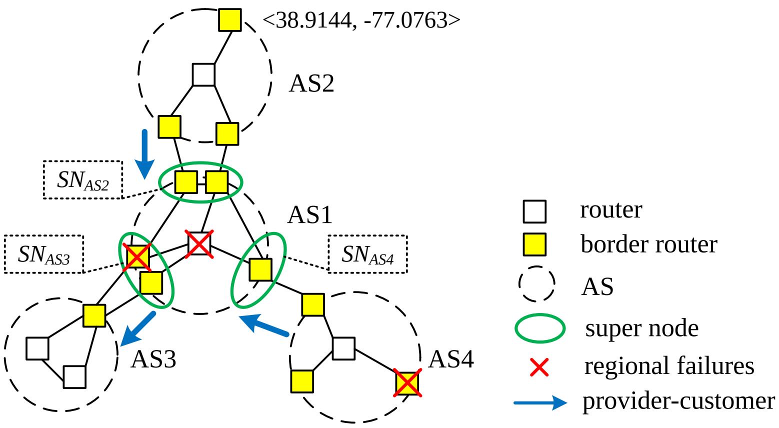

Fig. 2. An example of regional failures on inter-domain routing system

3.1 Topology Constructing

The first component is to construct an annotated topology of the Internet from several logical and physical topology data sources, including the AS topology, the AS relationships, the geo-locations of routers, the router and AS assignment and the router topology. The output annotated topology has two levels, which are AS level and router level. The AS level topology is presented as a graph $G = <V_{AS}, E_{AS}>$, where V_{AS} is the set of all ASes in the whole Internet, and E_{AS} is the set of AS links annotated by their business relationships, including provider-customer, customer-provider and peer-peer. Since BGP is a policy-based routing protocol and AS relationship is the essential factor to set routing policy, it is important to take this information into account. Whereas the router level topology is divided into multiple parts. Every part belongs to a single AS, and is also presented as a graph $G^{ASi} = <V_R^{ASi}, E_R^{ASi}>$, where V_R^{ASi} is the set of routers that *ASi* has, and E_R^{ASi} is the set of router links within *ASi*. Each router is annotated with its geographical location, presented as $<lat_r, lon_r>$ which are the combination of latitude and longitude of router *r*.

Fig. 2 illustrates the structure of a simple annotated topology. AS1, AS2, AS3 and AS4 construct the AS-level topology. The links AS2-AS1, AS1-AS3 and AS4-AS1 are annotated as provider-customer relationships. Within every AS, there are several routers constructing the router-level topology. Each of the routers is annotated with its location information, such as <38.9144, -77.0763>. This constructed topology is a basic foundation for the next two components in the model.

3.2 Intra-Domain Routing

The second component is to simulate the intra-domain routing process under regional failures in affected ASes. It takes the router-level annotated topology and geo-locations of failures as inputs, and provides the estimated effect of failures in terms of degradation of AS transit capability.

In REFER, if a regional failure occurs at location *L*, by querying the latitude and longitude of routers, all routers located at *L* will be taken down. Regional failures may break down multiple routers co-located in the region, and further affect multiple ASes that administer these routers. By identifying the affected ASes, we are able to transfer the problem from the physical space to the logical domains of the Internet. In each AS, routers are classified into two categories which are regular routers and border routers. Border routers are responsible for communicating with other ASes. Sometimes several border routers communicate with one neighbor AS. In this case, we define the set of these border routers as a super node associated with neighbor *ASi*, denoted as SN_{ASi}. In *ASj*, if all the border routers in SN_{ASi} are taken down due to the regional failure, the connectivity between *ASj* and *ASi* is no longer available. This is treated as a degradation of *ASj*'s transit capability, denoted as a two-tuples of ASes <*ASi*, *ASj*>. Moreover, if the fault routers disconnect every possible path between SN_{ASi} and SN_{ASk}, we consider it as another type of degradation of *ASj*'s transit capability denoted as a triple <*ASi*, *ASj*, *ASk*>. Currently, the two types of intra-domain routing protocol – distance vector routing protocol and link state routing protocol, are both based on the local optimal idea, that every router sends packets along with the shortest path on a certain distance scale. To this end, our model applies shortest path algorithm to find paths between any pair of routers within an AS, in order to simulate the routing process of IGPs in the intra-domain routing system. By calculating the degradation of transit capability associated with every affected ASes, we can evaluate how the geographical failures affect the Internet at a local scale.

For example, in **Fig. 2**, assume that regional failures disable three routers distributed in AS1 and AS4. For AS1, there are three super nodes SN_{AS2}, SN_{AS3}, and SN_{AS4} connecting to its neighbors. And no path is available between SN_{AS2} and SN_{AS3} because of the router faults. Hence AS1 is affected by the regional failures in terms of the degradation of its transit capability between AS2 and AS3, presented as <AS2, AS1, AS3>. This fine-grained method is more realistic, because the failures don't remove the entire AS1 from the topology. Moreover, the failure effect presented by the degradation of transit capability between ASes is the first fine-grained failure model rather than AS-level failure models. For example, previous research [6] classifies failures into three types: no logical link failure, single logical link failure, and multiple logical link failures. It is not able to describe the failure scenario in **Fig. 2**, because the regional failure neither breaks down any AS link, nor causes partial peering teardown and AS partition. From the intra-domain routing perspective, AS1 can still transmit traffic between AS2 and AS4, as well as AS3 and AS4. According to this method, we could evaluate the impact on affected ASes one by one. Faulty router in AS4 doesn't affect any connection between its neighbors.

3.3 Inter-Domain Routing

The third component is to simulate the inter-domain routing process in the whole Internet. The inputs include the AS-level annotated topology from the first component, the degradation of transit capability from the second component, and the routing policies adopted by every AS. The output is the resilience of the inter-domain routing system which is characterized by two metrics: change of reachability, and number of rerouting messages.

In the inter-domain routing system, the propagation of routing messages is constrained by topology of the Internet and routing policies. According to economic considerations of ASes, there are some common points of routing policies summarized by previous research [8, 9]. For import policies, if a BGP router receives routes to the same destination from different neighbors, it prefers route from customer over those from peer then from provider. Metrics such as path length and other BGP attributes are used in route selection if the preference is the same for different routes. This policy is known as 'customer-prefer'. For export policies, an AS does not transmit traffic between any of its providers or peers, which is called 'valley-free' property. Under these circumstances, connectivity does not mean reachability in the inter-domain routing system. In REFER, we assume that all ASes follow customer-prefer and valley-free policies. From intra-domain routing component, we find out the degradation of AS transit capability in terms of two- and triple-tuples of ASes when there are multiple breaks in the connectivity between ASes caused by regional failures. In the inter-domain routing component, we must label all these two- and triple-tuples of ASes as ‘unavailable’, and avoid them in route selection process. Note that the routing path from *ASi* to *ASj* is not necessarily the same as path from *ASj* to *ASi*, because the forward and reverse paths may be asymmetrical in the Internet. But the degradation of transit capability of an AS is symmetrical, i.e. if *ASi* is unable to transmit data traffic between *ASk* and *ASj*, <*ASk*, *ASi*, *ASj*> and <*ASj*, *ASi*, *ASk*> are both unavailable in inter-domain routing.

By comparing every inter-domain path before and after regional failures happen, we are able to evaluate how the failures affect resilience of the inter-domain routing system. In order to measure the difference quantitatively, we characterize the resilience by two metrics defined as follows.

Change of reachability: The degradation of AS transit capability entailed by regional failures could be harmful to the routing system for finding paths between every pair of source and destination. We define change of reachability, denoted as ΔR, to measure the difference of this capability.

$$\Delta R = \frac{\sum_{u,w\in V_{AS}} \chi_{uw} - \sum_{u,w\in V_{AS}} \chi'_{uw}}{\sum_{u,w\in V_{AS}} \chi_{uw}} \tag{1}$$

where χ_{uw} equals to 1 if there exist a path from u to w before failures occur. Otherwise, it equals to 0. Similarly, after failures occur, χ'_{uw} is 1 if there still exist a path between u and w. It equals to 0 if not. In this case, larger change of reachability indicates lower resilience of the routing system under the failures.

Number of rerouting messages: The most essential task for a routing system of networks is to make routing decisions. However, if large amounts of paths need to be rerouted around faulty routers, large amounts of BGP messages will be generated, sent and processed. In this case, the computational load on a router’s CPU increases dramatically, possibly exceeding the capacity of processors, then weakening the system’s ability of routing. So we propose the number of rerouting messages that received by every AS after regional failure to measure this effect. The number of rerouting messages received by u ($u \in V_{AS}$) is defined as

$$RM_u = \sum_{w\in V_{AS}} \delta_{uw} \cdot \rho(w) \tag{2}$$

where δ_{uw} is the number of paths from u to w that are different before and after failures. In our model REFER, paths are rerouted only due to regional faults. $\rho(w)$ is the number of IP prefixes in w. Since in BGP, the routing messages are generated regarding to every IP prefix. The more prefixes an AS has, the more routing messages it will generate when paths targeted to it need to be rerouted. The distribution of *RM* wrt. every AS reveals different effects of the failure on different AS. Generally speaking, more rerouting messages indicate lower resilience of the inter-domain routing system.

For the example in **Fig. 2**, there are 4 ASes, therefore 12 pairs of source-destination to examine. Due to the constraint of policy-compliant routing, no path is available between AS2 and AS4, for they violate the ‘valley-free’ policy. More precisely, AS1 is a customer of AS2 and AS4, and customer doesn’t transmit traffic for its providers. So before regional failure occur, there are 10 pairs of source-destination are reachable. After faulty routers break down, intra-domain routing component of REFER suggests that <AS2, AS1, AS3> is unavailable. So another two pairs of ASes, i.e. AS2-AS3 and AS3-AS2, are unreachable. Therefore ΔR is calculated as 0.2, i.e. (10-8)/10. Moreover, since AS2-AS3 is no longer reachable, AS2 will receive the route withdraws of every IP prefix in AS3; similarly, AS3 will receive the route withdraws of every IP prefix in AS2. The summation of these amount of withdraws is the number of rerouting messages after regional failures.

4. Simulations

To perform a case study of our model, we simulate a regional failure scenario that all routers locating at a city with important IXP are taken down. Then we build a simulator to simulate the routing dynamics described by REFER under this regional failure.

The data sources required by REFER are all inferred from the actual Internet data, which are considered as the most authoritative and comprehensive in the related research currently. The topology of the Internet and the AS relationships are from CAIDA's AS Relationships project in June 2012 [10]. The number of IP prefixes in every AS is calculated from the BGP routing tables collected by Route Views [11] and RIPE RIS [12]. And the geo-locations of routers, the router and AS assignment and the router topology income from CAIDA's ITDK (Internet Topology Data Kit) data set [13].

4.1 Regional Failure Scenario

We simulate a fault scenario taking down all the routers at a city where important IXPs of the Internet locate. An IXP is a physical infrastructure through which ISPs (Internet service providers) exchange Internet traffic between their ASes [14]. We believe IXPs are very important points connecting both physical and logical space of the Internet. Hence in this paper, we focus on the regional failure occurring on a city-level location where the most important IXP is set.

To perform the simulation, the first task is to evaluate the importance of cities in the world quantitatively. We propose a metric $I(loc_i)$ to measure the *interconnectedness* of loc_i as

$$I(loc_i) = \sum_{\exists r_B \in V_R^{ASj}, < lat_{r_B}, lon_{r_B} > \in loc_i} \log(D(ASj)) \tag{3}$$

where $\exists r_B \in V_R^{ASj}, < lat_{r_B}, lon_{r_B} > \in loc_i$ presents the condition that there exists a border router of ASj locating at loc_i. And $D(ASj)$ presents the degree of ASj, i.e. the number of its direct neighbors, which is a well-known metric for the importance of the AS in the routing system. This equation summarizes the log values of degree of ASes that have border routers locating at loc_i.

This equation is proposed based on the following observations. ASes interconnect with each other by border routers. And the degree of an AS indicates its connectedness in the routing system. But the degree of ASes in the Internet follows a 'power-law' distribution, i.e. a small number of core ASes have extremely high degree, whereas a large number of stub ASes have very low degree. To this end, we calculate the log value of AS degree to make them comparable.

The distribution of city interconnectedness is in **Fig. 3**, which also follows the 'power-law' distribution. **Fig. 4** shows the geographical distribution of its log-scale value. For example, the interconnectedness of a point whose value is 5 is at the scale of 10^5. Because of the scale-free property of the 'power-law' distribution, we plot the value at log-scale to make it clearer. The brighter color a city is painted, the higher interconnectedness it has. From the figure we can see that most interconnected cities locate in Europe and North America. The highest value belongs to city C in the U.S. (We conceal the city name for security consideration). In our following simulations, we make all routers in city C break down to simulate the most severe regional failure at city level.

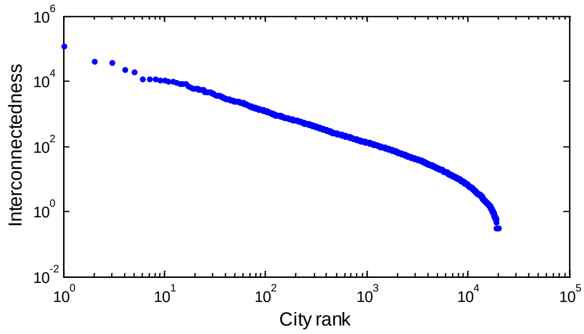

Fig. 3. The distribution of city interconnectedness

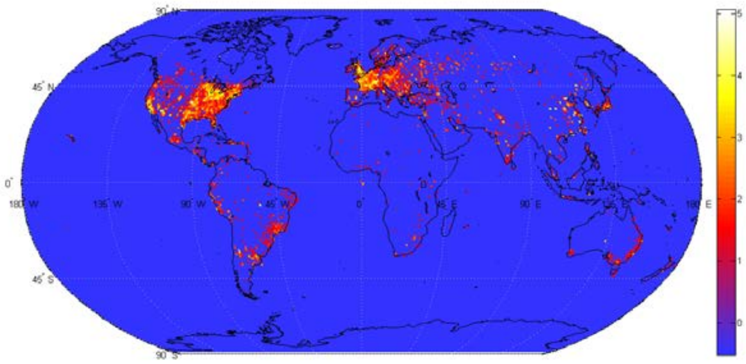

Fig. 4. The geographical distribution of city interconnectedness

4.2 Assessing Resilience under the Regional Failure

The process consists of three steps.

Step 1, we perform inter-domain routing simulation on every pair of source-destination normally to calculate the reachability. In addition, we record the paths from every source to every destination before the regional failure.

Step 2, assume that routers at city C are broken down, we perform intra-domain routing simulation in every affected AS to calculate the degradation of transit capability. Then we perform inter-domain routing simulation under this regional failure to record the reachability and paths for comparison.

Step 3, compare the reachability from step 1 and step 2 to calculate the change of reachability according to Eqn. 1. Then analyze the difference of paths due to rerouting after the failure to calculate the number of rerouting messages according to Eqn. 2.

A connected network with 41204 ASes and 121310 AS links is constructed to simulate the Internet based on the data sources mentioned above. According to the intra-domain routing component of REFER, under the regional failure scenario, 118 ASes are affected, i.e. 118 ASes deploy routers at city C. Among them, 27 ASes' transit capabilities are degraded. The numbers of their unavailable two-tuples and triple-tuples of ASes are shown in **Fig. 5**. From this result, we can find that there is one AS which is worst affected. Its AS number is AS20940. Since it has the most unavailable two- and triple-tuples of ASes, moreover, 72.5% of its routers locate at city C and fail in the regional failure scenario.

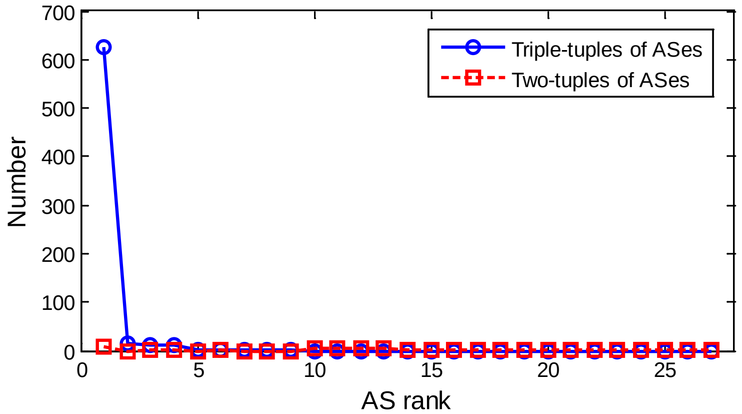

Fig. 5. The number of rerouting messages received by every AS

According to the inter-domain routing component of REFER, the change of reachability, i.e. ΔR, is 0.0024% after failure happens. This is a pretty low degradation of reachability. Further analysis shows that only AS31110 loses all the available paths to other ASes. All the other ASes can find at least one available path to any destination. Both of the two links connecting AS31110 to its neighbors (AS31110 to AS3549 and AS31110 to AS8121) are taken down by the regional failure, so it becomes an isolated island in the Internet.

Meanwhile, 41130 ASes need to process rerouting messages triggered by the failure. But the number of rerouting messages received by every AS varies dramatically. As shown in **Fig. 6**, the maximum number is 443654, while the minimum number is 1.

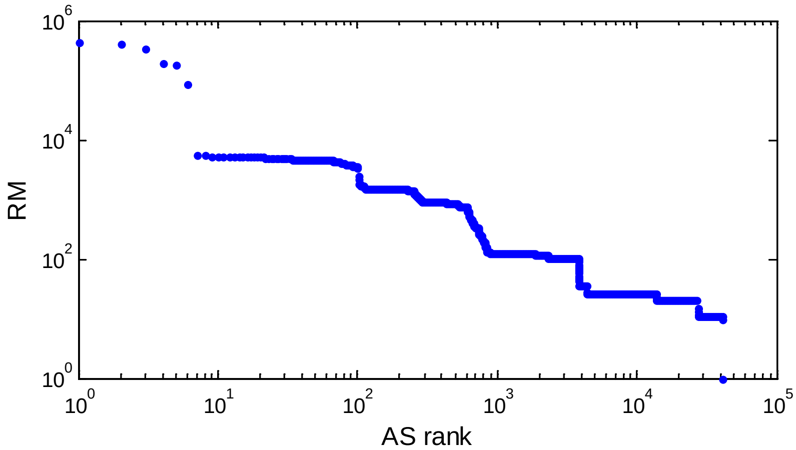

Fig. 6. The number of rerouting messages received by every AS

We cluster all the ASes as ‘heavily loaded’ and ‘lightly loaded’ based on the number of their receiving messages by applying K-means cluster algorithm. Heavily loaded cluster includes only three ASes, as shown in **Table 1**. These ASes lose one of their two links to neighbors due to regional failure. Therefore, large amount of rerouting messages are generated during the process of paths shifting from one faulty link to the other available one. It’s worth noting that the heavily loaded ASes are all stub ASes locating at the edge of the Internet. They do not provide traffic-transiting services for other ASes. Therefore, the huge volumes of rerouting messages are limited within a small scope of edge network, which hardly affect the core of inter-domain routing system.

By examining the two resilience metrics from the analysis results, we come to a conclusion that the inter-domain routing system is robust under our simulated IXP regional failure scenario.

Table 1. Heavily loaded ASes

AS number	Number of rerouting messages	AS type	AS degree	Number of unavailable two-tuples of ASes	Number of unavailable triple-tuples of ASes
AS15038	443654	Stub AS	2	1	0
AS22207	417473	Stub AS	2	1	0
AS16625	340320	Stub AS	2	1	0

5. Conclusion and Future Work

In this paper, we propose a model for regional failures in inter-domain routing system to assess the resilience of the Internet under disasters at a finer level, considering different routing policies of intra-domain and inter-domain routing systems, i.e., the shortest path algorithm of intra-domain routing and the policy-compliant algorithm of inter-domain routing. Moreover, we perform simulations on an empirical topology of the Internet to simulate a regional failure locating at a city with important IXP. We believe it is a very severe regional failure scenario because the location has the highest interconnectedness value, representing it is important to interconnect the network. However, analysis results show that the inter-domain routing system is robust under this city-level regional failure. Most ASes have at least one available path to any destination, and large amount of rerouting messages are limited within a small scope at the edge of the Internet.

We only simulate the regional failure at an IXP in our paper as a case study. In the future, we are going to extend the failure radius, and assess the relationship between the failure area and the resilience of the inter-domain routing system. Moreover, we will simulate different types of regional failures which locate at the PoP of Tier 1 AS, or at the important cable system, then apply REFER to assess resilience of the Internet.

References

[1] A. Popescu, T. Underwood and E. Zmijewski, "Quaking Tables: The Taiwan Earthquakes and the Internet Routing Table," in *Proc. of NANOG 39*, 2007.

[2] J. Cowie, "Japan Quake," http://www.renesys.com/blog/2011/03/japan-quake.shtml, 2016.

[3] A. Antony, L. Cittadini, D. Karrenberg, R. Kisteleki, T. Refice, T. Vest and R. Wilhelm, "Mediterranean Fiber Cable Cut (January-February 2008) Analysis of Network Dynamics," http://www.dia.uniroma3.it/~compunet/www/docs/2008-124.pdf, 2008.

[4] S. Neumayer, G. Zussman, R. Cohen and E. Modiano, "Assessing the Impact of Geographically Correlated Network Failures," in *Proc. of IEEE MILCOM' 08*, pp. 1-6, 2008. Article (CrossRef Link).

[5] A. Motter and Y. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E 66, 065102*, pp. 1-4, 2002. Article (CrossRef Link).

[6] J. Wu, Y. Zhang, Z. Mao and K. Shin, "Internet Routing Resilience to Failures: Analysis and Implications," in *Proc. of CoNEXT'07*, pp. 1-12, 2007. Article (CrossRef Link).

[7] W. Deng, M. Karaliopoulos, W. Muhlbauer, P. Zhu, X. Lu, B. Plattner, "k-Fault tolerance of the Internet AS graph," *COMPUTER NETWORKS*, vol. 55, no. 10, pp. 2492-2503, 2011. Article (CrossRef Link).

[8] L. Gao. "On inferring autonomous system relationships in the internet," *IEEE/ACM Transactions on Networking (ToN)*, vol. 9, no. 6, pp.733-745, 2001. Article (CrossRef Link).

[9] W. Deng, W. Muhlbauer, Y. Yang, P. Zhu, X. Lu, B. Plattner, "Shedding Light on the Use of AS Relationships for Path Inference," *Journal of Communications and Networks*, vol. 14, no. 3, pp. 336-345, 2012. Article (CrossRef Link).

[10] CAIDA, http://www.caida.org, 2016.

[11] Route Views, http://www.routeviews.org, 2016.

[12] RIPE RIS, http://www.ripe.net/ris, 2016.

[13] Macroscopic Internet Topology Data Kit (ITDK), http://www.caida.org/data/active/internet-topology-data-kit/, 2016.

[14] K. Xu, Z. Duan, Z. Zhang and J. Chandrashekar, "On Properties of Internet Exchange Points and Their Impact on AS Topology and Relationship," in *Proc. of Networking 2004*, pp. 284-295, 2004. Article (CrossRef Link).

Yujing Liu received her B.S., M.Sc. and Ph.D. degrees in Computer Science from the National University of Defense Technology, China, in 2007, 2009 and 2013 respectively. She is now a research assistant in the College of Computer from the NUDT. Her research interests include the Internet routing security and measurement.

Wei Peng received the M.Sc. and the Ph.D. degrees in Computer Science from the National University of Defense Technology, China, in 1997 and 2000 respectively. From 2001 to 2002, he was a research assistant in the College of Computer and the Science and Technology on Parallel and Distributed Processing Laboratory from the NUDT, then a research fellow from 2003. His major interests are Internet routing, network management, and mobile wireless networks.

Jinshu Su received his B.S. degree in Mathematics from Nankai University, China, in 1985 and the M.Sc. and Ph.D. degrees in Computer Science from the National University of Defense Technology, China, in 1988 and 2000, respectively. He is a professor in the College of Computer and the Science and Technology on Parallel and Distributed Processing Laboratory, NUDT. His research interests include network architecture, Internet routing and security.

Zhilin Wang received his B.S. and M.Sc. degrees in Computer Science from the National University of Defense Technology, China, in 2006 and 2009 respectively. He is now an engineer in the Education Department from the NUDT. His research interests include network security and management.