Internet Mapping at IP level

Santi García-Jiménez, PhD advisor: Eduardo Magaña
Universidad Pública de Navarra
Campus Arrosadia s/n, 31006 Pamplona
Tel: +34 948 166033, E-mail: {santiago.garcia, eduardo.magana}@unavarra.es

1. INTRODUCTION

Topology discovery is still nowadays an important challenge for research community. Internet growth has been very fast, and without too much control in how interconnection is provided. Networks were added to other neighbor networks but without sharing information about each other topology. Topology architecture is property of each enterprise and to know the network of the others can mean a quantitative disadvantage (security issues), so they try to keep the secret about their topology deployments.

From a researcher point of view, to know the real topology could mean a huge help at the time of improving the efficiency in actual routing algorithms or creating new ones. With real topology, research community can study the network behaviors closer to real models making more realistic studies.

Scientific community studies network models based on some topologies derived from how the network are organized. There are some approximations based on power laws and biases absence [1] and they are well known as good approximations, but an Internet map is not available to verify them.

There are also some topology approximations based on making different kind of tests. Some of them are based on traceroutes but these kind of probes do not show the real IP level topology because each IP are presented as a different single node in the resultant graph. There have been some great ideas to try joining different IP addresses belonging to the same router. Alias resolution schemes as Mercator [2] and Ally [3] are able to join some of the IP addresses to the same router. The first problem with them is that the tests are very far to give the total identification of routers and the second problem is that Internet is really big and some strategies to make all tests much faster must be developed. So this is a open research topic with many aspects to be discovered and improved.

The final objective of our research is to develop new techniques and ideas to create topology maps at IP level, representing Internet as a graph where nodes were routes. This means closer to reality.

2. STATE OF THE ART

The first step in topology discovery was made by Van Jacobson and his traceroute tool [4]. With the idea of using an incremental TTL, it was able to see all the IP addresses between one host and another. It is nowadays a very powerful tool to detect routing problems and the base for lots of researches in topology discovering.

If we focus on alias resolution problem, we can view two big advances in this field. First one is the Mercator identification method, and the second one is the Ally method.

The first one is based on the behavior of some routers when they have to send ICMP error packets. In many cases, the router will send all the ICMP error packets from the same interface and with the same source IP address to the source host for the packet which generated the error.

The second method is based in the behavior of IP identifier (IPID) field into IP layer [5]. To make this field different between packets, some routers use this field as an incremental counter. Ally use this behavior, sending UDP packets to a pair of IP addresses.

In order to prevent us to make all the possible tests to all possible pairs in the network there are some improving methods to reduce the number of tests. For example, we can focus on the TTL of the received packets and test only the IP addresses with a short TTL distance [6]. By this method we can reduce a lot the number of pairs to be tested. It can be also seen into literature another method based on IPIDs distances [7] to make the tests only to a more reduced set of IP addresses.

3. OUR WORK

We have been working in the implementation, evaluation and improvement of existing alias resolution methods. The first two methods which we implemented were Mercator and Ally. Then we proposed some improvements for those methods. First we made probing which more types of probing packets. For example, probing packets like ICMP ECHO REQUEST packets to receive from the router ICMP ECHO REPLY, like TCP ACK packets waiting for the TCP RESET packet from the router and we sent also ICMP TIMESTAMP REQUEST packets waiting for ICMP TIMESTAMP REPLY packets. The idea was to increase the number of responsive routers because due to packet filtering lots of the test that used UDP packets were lost.

A variation in the number of packets and the way to make the tests has been done. In our IPID based tests we have introduced a static time offset between probes. This static offset will make able to increase the number of packets to be sent to the candidate IP addresses to obtain more accurate tests.

Some studies of fault probability in Ally method has been done. First a theorical probability study with a simple model showed that the probability of error exists and it makes possible that some of the interfaces that not belong to the same router could be clustered in the same one. This study has been done over the classic Ally implementation based on

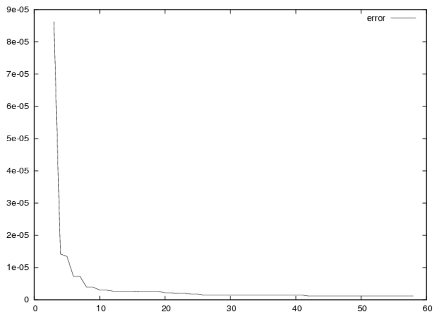

Figure 1: Error alias simulation

three packets.

Figure 1 shows the simulation results to check the behavior for increasing the number of packets in Ally's error probability. With 3 packets as used by Ally the probability of getting an error in alias identification is around 9 10^{-5}. This error can be reduced in two orders of magnitude with around 15 packets.

To make tests, we have used firstly a testbed, where all IP addresses, routers and links were well-known. In this environment, we were able to see if there was any kind of error in developing certain test. When all tests worked fine in our testbed without any kind of error in alias detection process, we used them into the real world using ETOMIC platform[8].

ETOMIC is a platform developed by a integrated project called Evergrow funded by European Union. It is a central networking experiment scheduler and has 18 nodes distributed around all Europe. The probes are synchronized by a GPS clock and they have two network interfaces. The first of them is an ethernet card and the second one is a Endace DAG card. The second card marks each packet sent with a high-precision timestamp and, with the GPS synchronization between probes, offers the possibility to make high precision one-way delay tests.

We have used this platform only as a way to feed our identification alias system with IP addresses. We have made Paris-traceroutes between each combination of nodes trying to make the connection network between them. Paris-traceroute [9] help us to know the real links between routers.

We are continuing the studies by using the Planetlab platform [10]. These nodes will be used to make Paris-traceroutes to obtain more IP addresses and also the probes will be used to make aliasing test using nodes as computation nodes.

Test	*True (%)*	*False (%)*	*Total (%) accumulated*
Mercator	0.017	0	0.017
Ally	0	15.037	15.041
IPID UDP	0.034	20.102	20.997
IPID TCP	0.024	21.468	31.609
IPID ICMP ECHO	0.033	32.700	48.585
IPID ICMP TSTAMP	0.0174	13.867	48.778

Table 1: Results for alias identification

In table 1, the alias identification results using the differents methods are presented. The last column is the result for applying the identification methods of certain row and all the methods in the rows before. Classical methods, Mercator and Ally, are able only to identify around 15% of pairs of IP addresses. Most of them are negative alias, and only a little percentage (0.017%) are positive alias. With our proposal, we improve the results up to almost 50% of pairs of IP addresses.

If we want to plot the entire Internet we have to face a big problem. The complexity of the number of tests in some of our aliasing methods. The better methods in a completeness view, are also the most complex in a implementation and network load view. They require more packets per test and these tests are made with pairs of IP addresses. We have a $O(n^2)$ complexity problem, with n the number of IP addresses. So if we increase the number of IP addresses to be tested we will increase much more the number of test to do. This kind of deficiencies must be faced doing the tests only to the pairs of IP addresses with most probability to be alias. This is our current and interesting work.

4. CONCLUSIONS

Alias resolution schemes allow to identify IP addresses belonging to the same routers. Improvements in the methods in the state of the art are being provided. First, improving the percentage of identification, using different kind of probing packets. Second, reducing the probing traffic needed to check for aliasing. Very good results are being obtained at this point.

5. REFERENCES

[1] Sevcan Bilir, Kamil Sarac, and Turgay Korkmaz. Intersection characteristics of end-to-end internet paths and trees. In *13TH IEEE International Conference on Network Protocols*, pages 378–390, November 2005.

[2] Jean-Jacques Pansiot and Dominique Grad. On routes and multicast trees in the internet. ACM SIGCOMM Computer Communication Review, 1998.

[3] N. Spring, R. Mahajan, and D. Wetherall. Measuring ISP topologies with Rocketfuel. In *Proc. ACM SIGCOMM*, 2002.

[4] V. Jacobson. Traceroute ftp://ftp.ee.lbl.gov/traceroute.tar.gz, October 1989.

[5] Rfc 791 internet protocol.

[6] N. Spring, M. Dontcheva, M. Rodrig, and D. Wetherall. How to resolve IP aliases. Tech. Report 04-05-04, Washington Univ. Computer Science, 2004.

[7] Hal Burch. Measuring an IP network in situ. Carnegie Mellon University, PhD thesis, ISBN 0-542-01549-8, 2005.

[8] D. Morato, E. Magaña, M. Izal, J. Aracil, F. Naranjo, F. Astiz, U. Alonso, I. Csabai, P. Haga, G. Somin, J. Seger, and G. Vattay. The European Traffic Observatory InfraestruCture (ETOMIC): A testbed for universal active and passive measurements. In *Proc. TRIDENTCOM 2005*, pages 283–289, 2005.

[9] Brice Augustin, Xavier Cuvellier, Benjamin Orgogozo, Fabien Viget, Matthieu Latapy Timur Friedman, Clemence Magnien, and Renata Teixeira. Avoiding traceroute anomalies with paris traceroute. In *6th ACM SIGCOMM*, pages 153–158, October 2006.

[10] Princeton University. http://www.planet-lab.org.