Root Cause Analysis

1. INTRODUCTION

What is root cause analysis and why is it important:

- Operators suddenly find that what is reachable is no longer reachable.
- Even connectivity between tier-1's is sometimes not unavailable (Amazon quote).
- Abrupt changes in performance: increased latency to certain parts of the Internet, increased load on certain network links, and so on.

Why is root cause analysis difficult and why have previous attempts not been successful:

- Changes in routing policy of a given AS could affect distant ASes.
- As we will show later, the entity responsible for a path change might appear neither on the old path nor on the new path.
- Knowledge as to what information is required for the analysis might not be know a-priori.
- Passive analysis of just BGP feeds is misleading. E.g., presense of BGP path does not imply an actual working path.
- Insufficient to have granularity of analysis at the level of ASes; network operators would prefer more detailed, possibily, even router level information.

Contributions:

- A theoretical analysis of what information is required to identify the root cause. We bound the set of ASes from which we need routing information in order to determine the root cause.
- Develop an active measurement system for finding the root cause. Leverage recent advances in measurements (such as reverse traceroute, sidecar, etc.) to develop a technique for finding the root cause for path changes to a given destination, as long as we have a measurement presence at the destination.
- Provide an approximate technique for finding the root cause for path changes to a destination when we don't have a measurement presense at the destination.
- Develop techniques to make the system work at scale.
- Provide results of deploying the system on Planetlab and possibly on Amazon EC2 nodes.

2. BOUNDING ROOT CAUSE ANALYSIS

Root cause detection is a hard problem as congested links and path dilation could be caused by decisions made at a relatively distant AS. We therefore need to develop a theory for root cause detection so as to come up with a candidate set of ASes that might have caused a routing change and the resulting congestion or dilation. We begin by considering the hypothesis proposed by Feldman et al. [4] with regards to identifying routing instabilities on the Internet. Their primary observation is that when routing changes occur on a path from S to T, the origin of the instability is either on the new path or on the old path. By considering multiple vantage points and multiple destinations, they propose a scheme that will help pinpoint the likely cause of a BGP update to one or two ASes in most cases.

We show that this hypothesis is in fact not valid and that routing changes could be due to actions taken by ASes that are neither on the old path nor on the new path. Consider for instance the example shown in Figure 1 and the routing of the path from S to T. Further, suppose that the link $H - I$ is down, resulting in $S \rightarrow F \rightarrow G \rightarrow T$ being the chosen path based on the traditional routing model identified by Gao-Rexford. (All inter-AS links are assumed to be provider-consumer links in this figure, with the provider placed above the consumer in the depiction.) When the link $H - I$ is restored and if F prefers the egress point e_2 over e_3 (because it is an early-exit), F adopts the path $F \rightarrow H \rightarrow I \rightarrow J \rightarrow T$. When F chooses this path, S uses its alternate path $S \rightarrow A \rightarrow B \rightarrow C \rightarrow T$ since it is of a shorter AS length. So the root cause which is the link $H - I$ is neither on the old path $S \rightarrow F \rightarrow G \rightarrow T$ nor on the new path $S \rightarrow A \rightarrow B \rightarrow C \rightarrow T$.

Having refuted the earlier hypothesis, we now propose an alternate theory that provides a more comprehensive charac-

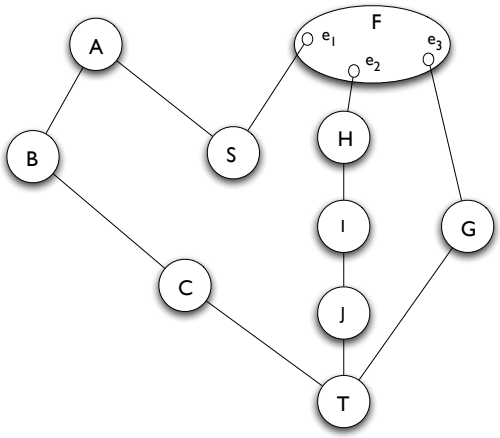

Figure 1: Example refuting root cause hypothesis put forth by Feldman et al.

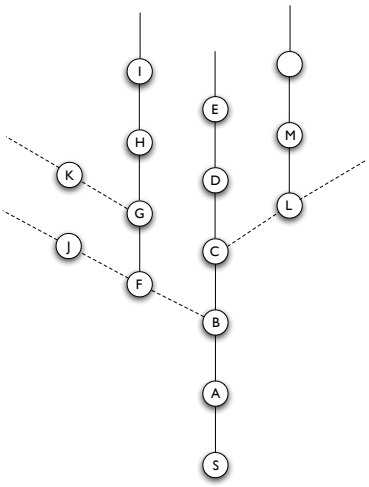

Figure 2: Sample topology for reasoning about root cause analysis.

terization that we show to be correct under the following set of reasonable assumptions.

- ASes use three criteria for path selection: (a) Economic utility (referred to as EU), where ASes prefer customer-provided paths over peer-provided ones and peer ones over paths through providers, (b) Network utility (NU) which optimizes for intradomain traffic (uch as early exit), and (c) Social utility (SU) wherein ASes prefers shorter AS paths. We assume that EU trumps NU which in turn trumps SU.
- At any point in time, only one routing event happens in the system, where the event could be a change in OSPF weights, a link going down, a link coming up, or an operator induced change. This assumption translates to a restriction on the granularity of observation, namely that the diagnosis system is invoked often enough to differentiate distinct events on the Internet.

We use the following notation. Let $O(S)$ be the old path from S to the target T at some point before the change occurs, and let $N(S)$ be the new path. Further, we abuse the notation a bit, by treating the paths as sets, generalizing the source to be a set of ASes instead of a single AS, and allowing for composition. We explain our notation using Figure 2, where we consider paths from various ASes to a target T (not shown in the figure). The old paths are those that are represented by solid lines and they go from bottom to top. After a routing event, some of the ASes change their routes to T by using links represented by the dashed lines (which branch off from the old paths by using the diagonal links). In this context, $O(S)$ is $\{S, A, B, C, D, E, ...\}$, and $N(S)$ is $\{S, A, B, F, J, ...\}$. Further $N(O(S))$ is the set of ASes that appear on the new paths originating from the ASes in $O(S)$, and $O(N(S))$ is the set of ASes that appear on the old paths originating from ASes in $N(S)$. For instance, $O(N(S))$ would contain the ASes $\{G, H, I\}$ since they are on the old path from F, which now appears on the new path $N(S)$; $O(N(S))$ would also contain $O(J)$, and so on. Similarly, $N(O(S))$ would contain L since C's new path to the target contains L.

THEOREM 1. *The AS responsible for a routing event is contained in the set* $N(O(S)) \cup O(N(S))$.

Proof: Given that it is not sufficient to consider just the old and new paths ($O(S)$ and $N(S)$) during root cause analysis, the above conjecture provides a tight bound on the set of other ASes that might have potentially initiated the routing changes. We prove this assertion now.

- We have already demonstrated that the root cause AS might be contained in $N(O(S))$. The following example demonstrates that the root cause can also be due to an AS in $O(N(S))$. Consider F in Figure 2. It uses the path $\{G, H, I\}$. Further, let it prefer this path over the path through J, either because of intradomain preferences or because of inter-AS peering preferences. Now if any link in the old path $\{G, H, I\}$ fails, F starts using the path through J. If the path through J is of much shorter length than the old path, then B would start using the path through F instead of its old path. More specifically, this happens when $length(B, F, J, \ldots, T) < length(B, C, D, E, \ldots, T$ $length(B, F, G, H, I, \ldots, T)$. So now we have a situation that the root cause is actually on $O(N(s))$.
- We now show that the root cause cannot be in the set $N(O(N(S))) - N(O(S)) - O(N(S))$. That is, it cannot include ASes such as K. The reasoning is as follows. Assume the contrary that the root cause is on the path $\{G, K, \ldots\}$. Further, after the routing event, let G start using the path through K because it prefers it over the old path due to any one of the criteria specified above. We can show that it will continue to export this new path to F. It will clearly do so because

the EU of the new path is at least as high as that of the old path (i.e, the peering relationship with K is as good as the one with H), and if it was exporting the path through H before, it will continue to export the new path through K. Now if F were to change its selected path from $\{G, H, I, \ldots\}$ to $\{F, J, \ldots\}$, it has to be based simply on SU. This is so because it had paths through J and G both before and after the event, and if it prefers the path through J over the one through G now, it must not be because of EU or NU; otherwise, it would have preferred the path through J in the past as well. This would mean that $length(F, G, H, I, \ldots) < length(F, J, \ldots) < length(F, G, K, \ldots)$. Since the only reason that B would prefers this new path $\{F, J, \ldots\}$, over its old path $\{C, D, E, \ldots\}$ must be because of SU, resulting in the constraint that $length(B, F, J, \ldots) < length(B, C, D, E, \ldots) < length(B, F, G, H, I, \ldots)$. This however contradicts the previous constraint on the lengths of the paths from F. Hence the root cause cannot contain a node such as K.

- Through a similar reasoning (which is omitted for brevity), we can show that the root cause cannot be in $O(N(O(S))) - N(O(S)) - O(N(S))$. That is, it cannot include ASes such as M.

The above theorem provides a tight bound on the set of ASes one would have to examine (or obtain information on) while investigating the root cause for routing events on the Internet. However, we have also expanded the set of potential ASes to examine as well as require substantially more routing information in order to determine the root cause.

3. TECHNIQUE FOR ROOT CAUSE DETECTION

Problem formulation: can we identify the root cause for path changes between a given pair of source and destination IPs. We assume that we have vantage points both at the source and the destination and also a distributed set of vantage points across the Internet. We will later relax the requirement that we need vantage points at both the source and the destination. We will also later consider the ability to scale up this analysis for a large number of source-destination pairs.

Theoretical analysis shows that we need two kinds of information:

- (a) New paths to the destination for the routing elements (ASes and routers) that appeared in the old path.
- (b) Old paths to the destination for the routing elements (ASes and routers) that appear on the new path.

Both types of information is challenging because:

- It might require vantage points at arbitrary locations.
- (b) is particularly challenging because it would require you to predict the path that will be adopted in the future, in order to monitor the paths currently being used by the routing elements on the future path.

Our technique:

- Use recently "reverse path" technique for finding the path from arbitrary IPs to a given destination. Keep this map refreshed at periodic intervals.
- Predict which paths might eventually be adopted, under the constraint that the root cause is not in one of the ASes appearing on the old path. Essentially, this boils down to predicting the set of alternate paths that exist between the source and the destination. Monitor paths from these IPs as well.

3.1 Routing Data from Arbitrary Sources

Quick summary of how we obtain the paths from a set of sources to a given destination. The reverse map provides the paths traversed by packets sent by these sources towards the given destination. This is essentially a quick summary of reverse-traceroute technique, along with a set of performance optimizations to make sure that we can refresh this map periodically.

3.2 Predicting New Paths from the Source to the Destination

Here the challenge is to come up with a reasonable set of paths that we need to monitor. Essentially do a mashup of historic routing information, generate an atlas, and compute feasible alternate paths. One possibility is to consider only policy compliant ones.

Experiment:.

Consider a set of traces from iPlane and identify how often new paths are simply paths that we have seen in the past. Also identify how often new paths are paths that can be "predicted" by composing known paths in a policy compliant way. Use the "3-tuple" check, in order to determine whether a path is policy compliant or not. The evaluation here is can we find a sweet spot regarding how many ASes we need to monitor while still obtaining broad coverage for future paths.

Experiment:.

Not sure this goes here, but how often do paths change and how do they change.

Stationarity experiments:.

- CDF per destination (using all iplane destinations, for 45 days)
  - how many path changes
  - how many intradomain path changes
  - how many interdomain path changes

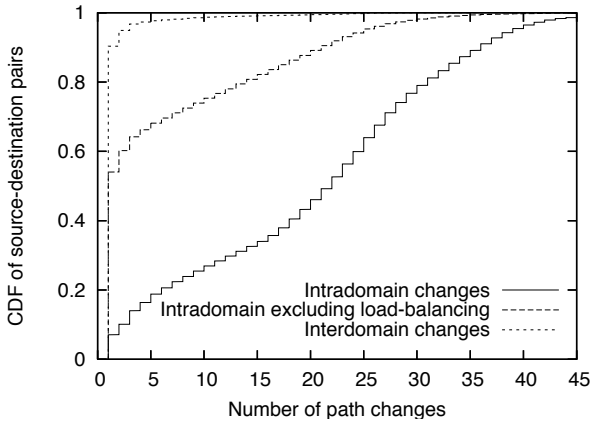

Figure 3: Path Stationarity.

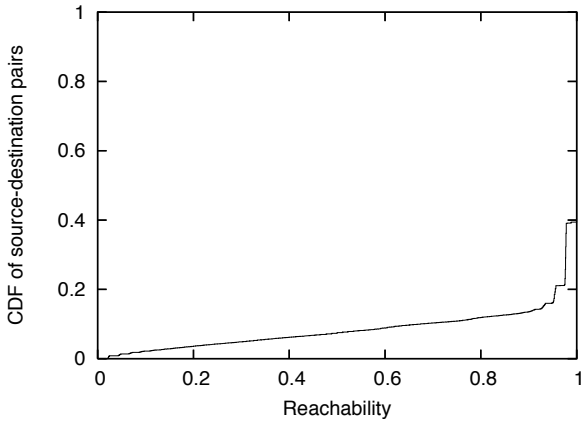

Figure 4: Reachability CDF.

  - how many intradomain parallel link changes

- are path changes predictable?
  - some path that we have seen before
  - some path that we can predict
- CDF of footprint of possible paths
  - based on previous paths
  - based on predictions

3.3 Datasets

- Daily traceroutes from PlanetLab to the rest of the world over a long period of time. (Essentially iPlane data.)
- Traceroutes every 10 minutes between pairs of PlanetLab node.
- Reverse map from routers to PlanetLab nodes, where the routers are those that we had observed before on paths between PlanetLab nodes.

4. SYSTEM DESIGN

5. EVALUATION

6. RELATED WORK

- [4] uses AS level information; is passive; assumes problems either on the old path or the new path.
- [1] similar to [4]. Correlation over time and across destinations.
- [18] is a passive + active monitoring technique for path changes, but does not provide root cause information.
- [6] focuses on reachability problems, provides rudimentary root cause information.
- [11] monitors routing data over time but does not analyze path changes across time.
- [16] discusses a measurement framework that could help with root-cause information.
- [14] augments BGP with root cause information.
- [17] focuses on a single AS and uses proprietary information.
- Other refs: [2], [3], [10], [12], [13], [9], [15], [8, 7], [5].

7. CONCLUSION

8. REFERENCES

[1] M. Caesar, L. Subramanian, and R. H. Katz. Root cause analysis of Internet routing dynamics. Technical report, Univ. of California, Berkeley, 2003.

[2] A. Dhamdhere, R. Teixeira, C. Dovrolis, and C. Diot. NetDiagnoser: Troubleshooting network unreachabilities using end-to-end probes and routing data. In *CoNEXT*, 2007.

[3] N. Feamster, D. G. Andersen, H. Balakrishnan, and M. F. Kaashoek. Measuring the effects of Internet path faults on reactive routing. In *SIGMETRICS*, 2003.

[4] A. Feldmann, O. Maennel, Z. M. Mao, A. Berger, and B. Maggs. Locating Internet routing instabilities. In *SIGCOMM*, 2004.

[5] Y. Huang, N. Feamster, A. Lakhina, and J. J. Xu. Diagnosing network disruptions with network-wide analysis. In *SIGMETRICS*, 2007.

[6] E. Katz-Bassett, H. Madhyastha, J. John, A. Krishnamurthy, D. Wetherall, and T. Anderson. Studying blackholes in the Internet with Hubble. In *Proc. of Networked Systems Design and Implementation*, 2008.

[7] R. Kompella, J. Yates, A. Greenberg, and A. Snoeren. Detection and localization of network black holes. In *INFOCOM*, 2007.

[8] R. R. Kompella, J. Yates, A. Greenberg, and A. C. Snoeren. IP fault localization via risk modeling. In *NSDI*, 2005.

[9] C. Labovitz, A. Ahuja, and M. Bailey. Shining Light on Dark Address Space. `http://www.arbornetworks.com/dmdocuments/dark_address_space.pdf`.

[10] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian. Delayed internet routing convergence. In *Proc. of ACM SIGCOMM*, 2000.

[11] H. V. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani. iPlane: An Information Plane for Distributed Services. In *Proc. of Operatings System Design and Implementation*, 2006.

[12] R. Mahajan, D. Wetherall, and T. Anderson. Understanding BGP misconfiguration. In *SIGCOMM*, 2002.

[13] Z. M. Mao, R. Bush, T. G. Griffin, and M. Roughan. BGP beacons. In *IMC*, 2003.

[14] D. Pei, M. Azuma, D. Massey, and L. Zhang. BGP-RCN: Improving BGP convergence through root cause notification. *Computer Networks*, 48(2):175–194, 205.

[15] A. Shaikh and A. Greenberg. OSPF monitoring: Architecture, design and deployment experience. In *NSDI*, 2004.

[16] R. Teixeira and J. Rexford. A measurement framework for pin-pointing routing changes. In *ACM SIGCOMM workshop on Network Troubleshooting*, 2004.

[17] 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 *NSDI*, 2005.

[18] M. Zhang, C. Zhang, V. S. Pai, L. Peterson, and R. Wang. PlanetSeer: Internet path failure monitoring and characterization in wide-area services. In *OSDI*, 2004.