Combining Routing and Traffic Data for Detection of IP Forwarding Anomalies

Matthew Roughan* Tim Griffin† Morley Mao‡ Albert Greenberg§ Brian Freeman¶

Categories and Subject Descriptors: C.2.3 Network Monitoring, C.4 Reliability, availability, and serviceability.

General Terms: Algorithms, Management, Reliability.

Keywords: Network anomaly detection, routing, BGP, traffic, SNMP.

ABSTRACT

IP forwarding anomalies, triggered by equipment failures, implementation bugs, or configuration errors, can significantly disrupt and degrade network service. Robust and reliable detection of such anomalies is essential to rapid problem diagnosis, problem mitigation, and repair. We propose a simple, robust method that integrates routing and traffic data streams to reliably detect forwarding anomalies. The overall method is scalable, automated and self-training. We find this technique effectively identifies forwarding anomalies, while avoiding the high false alarms rate that would otherwise result if either stream were used unilaterally.

1. INTRODUCTION

Anomaly detection is useful in network management for a range of applications, from detecting security threats (e.g. denial of service attacks), to detecting vendor implementation bugs, network misconfigurations or faults. One wishes to detect times where the network is behaving abnormally, as action may then be required to correct a problem. Anomaly detection can be particularly useful in the context of reliability. Reliability is a critical objective in large IP networks, but many factors (for instance code bugs) are outside of an operator's ability to control. An alternative to preventing outages is to rapidly recover from these [1, 2]. In order to recover quickly, one must detect and localize a problem quickly.

However, while detection and alarming on real problems is important, it is equally important to keep the rate of false alarms low. A high false alarm rate results in genuine events being lost in the "snow" of false events. Statistical anomaly detection tests are run often (e.g., every five minutes), on large networks (with ten's of thousands of links), and so even a seemingly low false alarm rate may result in enough false alarms to overwhelm network operations staff. In the worst case, false alarms undermine anomaly detection, as operations staff tire of reacting to false alarms, and ignore or turn the system off entirely.

IP forwarding anomalies represent a large class of network anomalies, that relate to problems in forwarding packets to their destinations. More precisely, a *forwarding anomaly* is a period during which a significant number of packets fail to successfully exit the network at an appropriate point. Network component failures (line card, optical amplifier, or router outages, and fiber cuts) are not usually within the class of such anomalies. During such events, IP traffic is rerouted along alternate paths, resulting in at most a short transient anomaly while the routing protocols reconverge. Also, such failures are typically isolated, and easily detectable via other means, e.g. the Simple Network Management Protocol (SNMP). However, as we note below, component failures may trigger some larger network error, or occur simultaneously.

Forwarding anomalies can be the result of several problems:

- **Bugs:** Bugs in router software may cause forwarding problems that do not register via any hardware alerts, or may further be related to bugs in the instrumentation itself.
- **Misconfigurations:** The IP control plane — the distributed protocols that coordinate the building of forwarding tables throughout the network — is very complex. In such systems it is hard for an operator to understand the state of the system, and therefore the possible impacts of their actions [2]. The result is that routers may be configured in such a way that packets do not reach their destinations, even though the network may appear to be working normally. Such misconfigurations are not entirely under the control of a single operator, as BGP allows network operators to misconfigure their systems in a way that may impact another network. Note that in [3] the authors found that operator errors in the form of misconfiguration was the major cause of service affecting outages, and BGP in particular has been seen to be hard to administer.
- **Cascading network failures:** In a cascading network failure, a simple failure (such as that of a line card) results in widespread disruption of the network. Although, the possibility of such a collapse is not anticipated in the Internet, such failures are difficult to predict, or control, and certainly have been observed in other network systems, for instance the power grid in North America in August 2003, and in the telephone network [4].
- **Latent errors:** It is possible to have latent errors: problems that are not significant until another error triggers them. A simple example might be a backup path that has been misconfigured, so that it does not work. Without careful testing such a problem might not come to light until after failure of the primary link. The failure of the primary link would be dealt with using normal procedures for detection and re-mediation, but without anyone realizing that the backup path was also failed, they might not give this task the priority it requires.

*University of Adelaide, <matthew.roughan@adelaide.edu.au>
†Intel Research Cambridge <tim.griffin@intel.com>
‡University of Michigan <zmau@eecs.umich.edu>
§AT&T Research, <albert@research.att.com>
¶AT&T Labs, <bdfreeman@att.com>

SIGMETRICS/Performance'04, June 12–16, 2004, New York, NY, USA.
ACM 1-58113-664-1/04/0006.

- **Exogenous factors:** Although Networking equipment is generally held in tightly controlled environments, with redundant power supplies, and A/C, rare events, for instance the Sept 11 attack on the World Trade Center, are large enough to effect a large part of the network. Obviously, detection of such impacts will be secondary to the event in question, but may none-the-less be useful in order to quickly assess the scale of the impact.
- **Simultaneous failures:** Most networks plan for single component failures, for instance, by providing pairs of redundant links. Given independent failures (consideration must be given to shared risk link groups when making such assumptions [5]) simultaneous failures should be unlikely, but can occur, with severe consequences, e.g. [6].

A consistent property in the above problems is that the standard methods for detecting network problems, for instance SNMP traps, syslog messages, etc., either do not detect such events, or see the true extent of the problem. Understanding the extent of a problem quickly is important in order to prioritize the event appropriately.

A large outage of a major tier-1 provider that happened on October 3rd 2002 [7], was found to have a large impact on routing data (from a BGP monitor) data, and traffic data (from SNMP measurements), and this motivated the investigation of using these data sources, in conjunction, to detect and localize such anomalies. Each data source provides a different view of such anomalies, with both having problems in data quality and in missing causality information that lead naturally to false alarms. On the other hand, if such problems are suitably uncorrelated in two data sources, then the false alarm rate can effectively be diminished by alarming only if both data sources indicate the anomaly concurrently.

First, we transform each data set individually to create useful anomaly metrics. Though SNMP usage data is relatively simple — the number of packets or bytes that traverse an interface between successive polling intervals — operational measurements for large networks can be relatively complex and noisy. We use two methods to extract the anomaly indicators from this data: a standard technique called Holt-Winters[8], and a second novel method based on a decomposition of the traffic into a trend, a periodic component, and stochastic components comprising normal variation, and anomalies (similarly to [9]). BGP dynamic updates, on the other hand, provide a rich, high-dimensional data source, with considerable volatility. Here, to extract a useful anomaly indicator, we transform the raw data to simulate and track BGP tables at locations throughout the network. We then form the dynamic count of the number of routes in these tables satisfying a given predicate, and use a modified exponentially weighted moving average technique [10] to signal anomalies. Last, we correlate the SNMP and BGP anomaly indicators in time to produce a combined indicator.

2. RESULTS

The anomaly detection techniques were tested on a large volume of data from am operating tier-1 network. We first show, in Figure 1, an example set of data, with anomalies in the individual datasets shown, along with the time of the real anomaly: the failure of a peer. During this failure, the peer dropped traffic along its peering links in a number of locations. In the Figure, we focus on a PoP where nearly half of the traffic (and corresponding routes) arose from that peer, and so the failure stands out clearly. However, the failure was also detected in a number of other locations. The example is highly illustrative for two reasons. Firstly, it shows the the fact that the two datasets give good indications of the fault. Secondly, it shows a number of false alarms in one of the datasets, that are avoided using the pair.

We have performed statistical study of the results, to find that firstly, the methods (using either Holt-Winters, or the Decomposition technique on the SNMP data, and the EWMA on the BGP data) had perfect detection of the known events, but that Holt-Winters had a slightly larger false alarm rate. However, the key point of the results was a dramatic reduction in the false alarm rate through using both sets of data. We still retain the perfect detection probability, but with a reduction in false alarms by more than a factor of one hundred, to the point where the results are operationally useful.

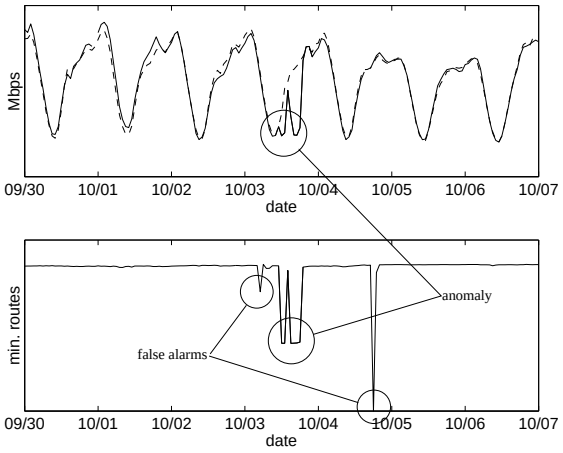

Figure 1: Example of joint anomaly detection (SNMP shown in top plot, BGP in lower plot).

3. CONCLUSION

This paper has described an important class of network anomalies — forwarding anomalies — and specific methods for combining routing and traffic data to perform accurate forwarding anomaly detection. The method is very simple, and so despite its power, there are opportunities for improvement: for instance, by including new dataset, e.g. OSPF data, netflow, router logs, or active probes. The method might also be improved by new algorithms for detecting anomalies (e.g. see [11]), or for combining the data from such.

4. REFERENCES

[1] A.Brown and D. A. Patterson, "To err is human," in *Proceedings of the First Workshop on Evaluating and Architecting System dependability (EASY '01)*, (Gteborg, Sweden), 2001.

[2] D. Patterson, A. Brown, P. Broadwell, G. Candea, M. Chen, J. Cutler, P. Enriquez, A. Fox, E. Kiciman, M. Merzbacher, D. Oppenheimer, N. Sastry, W. Tetzlaff, J. Traupman, and N. Treuhaft, "Recovery-oriented computing (roc): Motivation, defi nition, techniques, and case studies," Tech. Rep. UCB//CSD-02-1175, UC Berkeley Computer Science, 2002.

[3] D. Oppenheimer, A. Ganapathi, and D. A. Patterson, "Why do Internet services fail, and what can be done about it?," in *4th Usenix Symposium on Internet Technologies and Systems (USITS'03)*, 2003.

[4] D.J.Houck, K.S.Meier-Hellstern, F.Saheban, and R.A.Skoog, "Failure and congestion propagation through signalling control," in *Proceedings of the 14th International Teletraffic Congress (ITC-14)* (J. Labetoulle and J. W.Roberts, eds.), vol. 1a, pp. 367–376, Elsevier, 1994.

[5] J. Strand, A. Chiu, and R. Tkach, "Issues for routing in the optical layer," *IEEE Communications Magazine*, February 2001.

[6] Nanog mailing list `http://www.cctec.com/maillists/nanog/historical/0005/msg00073.html`, 5th May 2000.

[7] Nanog mailing list: `http://www.cctec.com/maillists/nanog/historical/0210/msg00058.html`, 3rd October 2002.

[8] J. D. Brutag, "Aberrant behavior detection and control in time series for network monitoring," in *Proceedings of the 14th Systems Administration Conference (LISA 2000)*, (New Orleans, LA, USA), USENIX, December 2000.

[9] M. Roughan, A. Greenberg, C. Kalmanek, M. Rumsewicz, J. Yates, and Y. Zhang, "Experience in measuring Internet backbone traffi c variability: Models, metrics, measurements and meaning," in *Proceedings of the International Teletraffic Congress (ITC-18)*, 2003.

[10] S. H. Steiner, "Grouped data exponentially weighted moving average control charts," *Applied Statistics*, vol. 47, no. 2, 1998.

[11] P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffi c anomalies," in *ACM SIGCOMM Internet Measurement Workshop*, (Marseilles, France), November 2002.