Interdomain Routing Streams

Timothy G. Griffin* Zhuoqing Morley Mao†

Abstract

Dynamic routing in the global Internet is currently performed by the Border Gateway Protocol (BGP). Initialization of a BGP session results in a full routing table being exchanged — currently about 130,000 routes. After initialization, BGP speakers send only *deltas* to their neighbors. Once timestamps are added to a stream of BGP deltas, it can be thought of as an append-only relation. Many queries useful in network monitoring can then be expressed as continuous queries over this data stream. In this abstract we briefly describe these streams as well as several public sources of data.

1 BGP and Network Monitoring

The Border Gateway Protocol (BGP) [7, 3] is the only dynamic routing protocol used to maintain reachability between autonomously administered networks on the global Internet. Initialization of a BGP session results in a full routing table being exchanged — currently about 130,000 routes. After initialization, BGP speakers send only *deltas* to their neighbors.

BGP routing streams are designed to allow BGP speaking routers to maintain timely information about the reachability of IP address ranges. However, tapping into this stream of data has proved very valuable to network operators, engineers, and researchers interested in monitoring the global dynamics of the IP routing system. In particular, an Internet Service Provider (ISP) may want to monitor its customer routes and its own address space very carefully. Applications of this kind need to process streams of BGP messages arriving from dozens of BGP speakers in a network in near real-time.

In this abstract we will refer to the publicly available BGP data archived at Route Views [1] and RIPE [6]. However, the reader should keep in mind that the network management applications we are most interested in are driven by near real-time data available *inside* large ISP networks. Typically, ISPs consider such data to be proprietary, since it contains customer and infrastructure information that is filtered out before being sent to external BGP neighbors, and to BGP archive sites such as Route Views and RIPE.

The Route Views BGP monitor collects update streams from 25 BGP speaking neighbors. Typically, Route Views collects five to six million updates per day. This is approximately the same order of magnitude of updates that might be collected inside a large ISP with BGP streams arriving from 25 large metropolitan regions. Figure 1 shows four updates sent to Route Views from AT&T on March 26, 2003. A *type* of "A" represents and announcement, while a "W" represents a withdrawal. The *prefix*, such as 217.12.112.0/20, represents a range of IP addresses. The *AS path* is a BGP attribute that records the Autonomous Systems that an announcement has traversed. (BGP records actually contain more attributes used to implement policy-based routing, but for simplicity we ignore them here.) The timestamp has a granularity of one second, and these updates arrived within the same timestamp.

BGP Streams can be thought of as an append-only relation, and many queries useful in network monitoring can then be expressed as continuous queries over this data stream [8, 4, 2].

Update rate. The simplest type of continuous query is a count of the number of updates received during some window of time. For example, Figure 2 shows the BGP update count per second from Route Views during the "SQL Slammer Worm" attack of January 25, 2003. Note that there is a sudden sharp increase in the number of BGP updates. The reason that a worm might impact BGP routing is a bit involved, but it is primarily due to saturation of links at the edge of the network resulting in dropped BGP messages, which in turn causes BGP sessions to reset and BGP speaking routers to withdraw routes. In general, ISPs are very interested in monitoring the stability of routes sent from their customers.

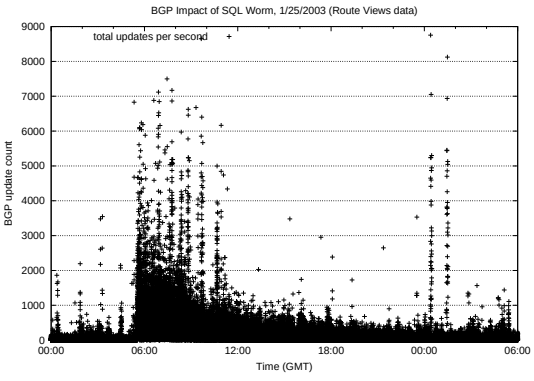

Figure 2: Update counts during SQL Slammer worm

Aggregate stability measures. A more sophisticated measure of route instability can be based on the route penalty metric associated with BGP's route flap damping mechanism [9, 5]. Each route is associated with a penalty that is increased each time the route changes. This penalty decays ex-

*AT&T Labs – Research, Florham Park, NJ, USA. E-mail: griffin@research.att.com.

†Computer Science Division, University of California at Berkeley, USA. E-mail: zmao@eecs.berkeley.edu.

timestamp	type	prefix	AS path
1048665376	A	217.12.112.0/20	7018 3356 8220 12878 5606 15471 25454
1048665376	W	212.49.85.0/24	
1048665376	A	12.27.216.0/24	7018 1239 14793 26809
1048665376	A	12.27.217.0/24	7018 1239 14793 26809

Figure 1: Sample updates from Route Views.

ponentially. Figure 3 shows aggregated penalty values during the "SQL Slammer Worm" attack. Note that there is a sharp increase in the aggregate penalty value around 06:00 GMT on January 25, 2003, when the attack just started. Such change can be used as an alarm to help network operators quickly recognize the problem.

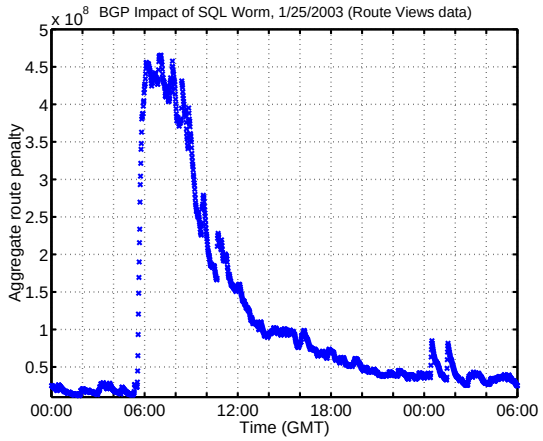

Figure 3: RFD Penalty during SQL Slammer worm

BGP table. The BGP table contains "best routes" to all of the destinations it has learned. Given a continuous BGP stream, starting at some time t in the past, sent from neighboring router R, we can construct that portion of R's BGP table that has changed since time t. If a BGP session reset has occurred since t, then we can reconstruct the entire BGP table (since a router must send its entire table when a sessions is reestablished after a reset). This table can be thought of as a materialized view of the BGP update stream. One simple query over this view is the number of routes in the table. Figure 4 shows BGP table size for several Route Views neighbors during the "SQL Slammer Worm" attack. Note that there is a sudden sharp drop in the number of routes in these BGP tables. Since this is seen across a large number of sources, it can be interpreted as a global disruption in the global routing system and could be seen as an early warning sign of trouble on the Internet.

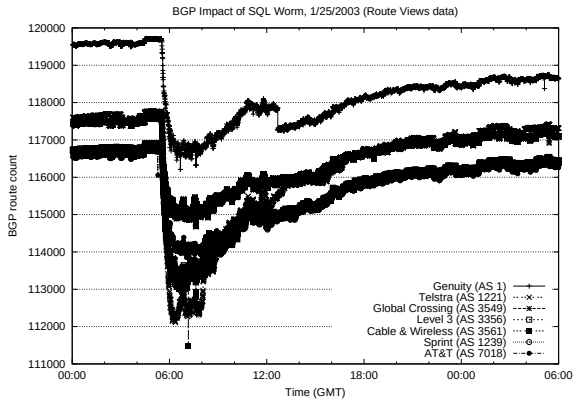

Figure 4: Table size during SQL Slammer worm

References

[1] University of Oregon Route Views Archive Project. `www.routeviews.org`.

[2] Brian Babcock, Shivnath Babu, Mayur Datar, Rajeev Motwani, and Jennifer Widom. Models and issues in data stream systems. In *Proceedings of Symposium on Principles of Database Systems (PODS 2002)*.

[3] B. Halabi. *Internet Routing Architectures*. Cisco Press, 1997.

[4] Ling Liu, Calton Pu, and Wei Tang. Continual queries for internet scale event-driven information delivery. *Knowledge and Data Engineering*, 11(4):610–628, 1999.

[5] Zhuoqing Morley Mao, Ramesh Govindan, George Varghese, and Randy H. Katz. Route flap damping exacerbates internet routing convergence. In *Proceedings of ACM SIGCOMM 2002*.

[6] Ripe NCC. Routing Information Service Raw Data. `http://abcoude.ripe.net/ris/rawdata/`.

[7] Y. Rekhter and T. Li. A border gateway protocol. RFC 1771 (BGP version 4), 1995.

[8] Douglas Terry, David Goldberg, David Nichols, and Brian Oki. Continuous queries over append-only databases. In *Proceedings of ACM SIGMOD 1992*.

[9] C. Villamizar, R. Chandra, and R. Govindan. BGP Route Flap Damping. RFC 2439, 1998.