BGPStream: a framework for historical analysis and real-time monitoring of BGP data

Chiara Orsini, Alistair King, Alberto Dainotti
alberto@caida.org

Center for Applied Internet Data Analysis
University of California, San Diego
Country-wide Internet outages in Iraq that the government ordered in conjunction with the ministerial preparatory exams - Jul 2015
Outage of AS11351 (Time Warner Cable LLC)
September 30, 2015
Hijacks: detection of MITM BGP attacks

- Normal path
- Hijacked path
- Normal path used to complete the attack

Source (poisoned) \( S \)
Destination (hijacked prefix) \( D \)
Attacker \( A \)

www.caida.org/funding/hijacks/
IODA SYSTEM DIAGRAM
(toy diagram)
IODA SYSTEM DIAGRAM
(toy diagram)

Center for Applied Internet Data Analysis
University of California San Diego
The “prefix-monitor” plugin (distributed with source) monitors a set of IP ranges as they are seen from BGP monitors distributed worldwide:
- how many prefixes reachable
- how many origin ASes
- generates detailed logs

Example: studying AS path inflation

How many AS paths are longer than the shortest path between two ASes due to routing policies? (directly correlates to the increase in BGP convergence time)

```python
from _pybgpstream import BGPStream, BGPRules, BGPReason
from collections import defaultdict
from itertools import groupby
import networkx as nx

stream = BGPStream()
as_graph = nx.Graph()
rec = BGPRecord()

collections = defaultdict(lambda: defaultdict(lambda: defaultdict(lambda: defaultdict(defaultdict))))
safe_stream = collections

for elem in stream:
    hop = {k: g for k, g in groupby(elem.fields['as-path'].split(' '))}
    length = len(hop[-1])
    hop[len(hop[-1])] = hop[-1]
    hop = hop.values()

    monitor = str(elem.peer_addr)
    origin = elem['as']

    if length < min((filter(lambda x: bgp_lens[monitor][origin] + '-', x) for x in hop if x == length)):
        bgp_lens[monitor][origin][length] += 1
        bgp_lens[monitor][origin][length], bgp_lens[monitor][origin][length][length] += 1

    bgp_lens[monitor][origin][length] += 1

    if monitor not in bgp_lens[monitor][origin].keys():
        bgp_lens[monitor][origin][length][length] += 1

    print monitor, origin, bgp_lens[monitor][origin], safe_stream
```

30 LINES OF PYTHON CODE
Center for Applied Internet Data Analysis
University of California San Diego
1. A web service ("BGPStream Broker")
   • enables SIMPLE access to LOTS of heterogeneous BGP sources
2. LibBGPStream:
   • Acquires the data and provides to upper layers a realtime stream of BGP data
   • makes it SIMPLE to process data from LOTS of heterogeneous BGP sources
3. Command-line tools and APIs in C and Python
• Design goals:
  - Efficiently deal with large amounts of distributed BGP data
  - Offer a time-ordered data stream of data from heterogeneous sources
  - Support near-realtime data processing
  - Target a broad range of applications and users
  - Scalable
  - Easily extensible

BGPStream: a software framework for live and historical BGP data analysis
Chien-Chuan, Alexander King, Alberto Darwiche
CAIDA, UC San Diego
**NO MANUAL DOWNLOADS**

*libBGPStream talks to the broker and gets the data*

```
stream.add_filter('record-type', 'ribs')
stream.add_filter('collector', 'route-views.sfmix')
stream.add_interval_filter(1445306400, 1445306402)
```

```
bgpstream_add_filter(bs, BGPSTREAM_FILTER_TYPE_COLLECTOR, "rrc06");
bgpstream_add_filter(bs, BGPSTREAM_FILTER_TYPE_COLLECTOR, "route-views.jinx");
bgpstream_add_filter(bs, BGPSTREAM_FILTER_TYPE_RECORD_TYPE, "updates");
bgpstream_add_interval_filter(bs, 1286705410, 1286709071);
```

```
$ bgpreader -w 1445306400,1445306402 -c route-views.sfmix -t updates
$ bgpcorsaro -w 1445306400,1445306402 -p ris
```

---

**Center for Applied Internet Data Analysis**

**University of California San Diego**
libBGPStream keeps retrieving data as it becomes available

```python
stream.add_filter('record1type', 'ribs')
stream.add_filter('collector', 'route-views.sfmix')
stream.add_interval_filter(1445306400, 11)

cdp.add_filter(BGPSTREAM_FILTER_TYPE_COLLECTOR, 'rrc06');
bgpstream.add_filter(BGPSTREAM_FILTER_TYPE_COLLECTOR, 'route-views.jinx');
bgpstream.add_filter(BGPSTREAM_FILTER_TYPE_RECORD_TYPE, 'updates');
bgpstream.add_interval_filter(bs, 1286705410, BGPSTREAM_FOREVER);
```

Center for Applied Internet Data Analysis
University of California San Diego
Access BMP-generated data from BGPStream

Data available with ~1 min latency

Developed in collaboration with Tim Evens @ Cisco and John Kemp @ Route Views

Experimental integration using OpenBMP to export MRT files (native BMP support planned for BGPStream).
BMP DATA SOURCES

Data Providers

- Current BMP feeds provided courtesy of Route Views, Cisco, and Randy Bush

Center for Applied Internet Data Analysis
University of California San Diego
BMP DATA SOURCES

don’t need to download a new BGPStream version

• Available to all existing BGPStream installs
  - Use filter to select data from provider “caida-bmp”
  - E.g. bgpreader -p caida-bmp -w 1453912260
• send us a bmp feed!
  - contact bgpstream-info@caida.org
THANKS

bgpstream.caida.org