BGPMON.IO: THE MANY NEW FACES OF BGPMON

Colorado State University
Spiros Thanasoulas and Christos Papadopoulos
NANOG 69, Feb 6-8 2017, Washington DC

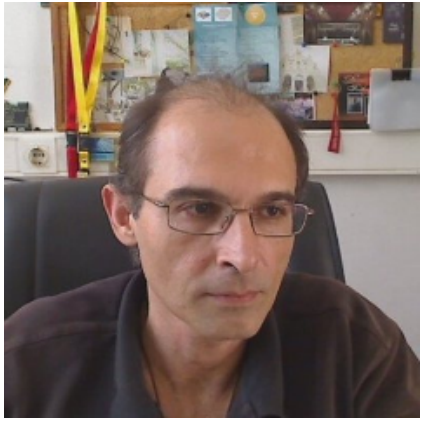
Work supported by NSF #CNS1305404, DHS #D15PC00205,
Cable Labs and the Australian Government

Colorado State University

The Team

Anant Shah

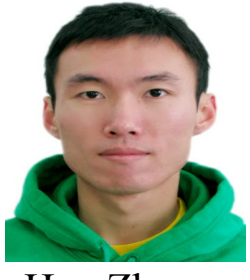
Spiros Thanasoulas



Dimitris Kounalakis

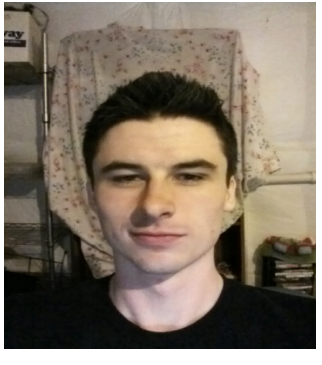
Christos Papadopoulos

Will Yingling



Han Zhang

Dan Rammer



Tyler Scott

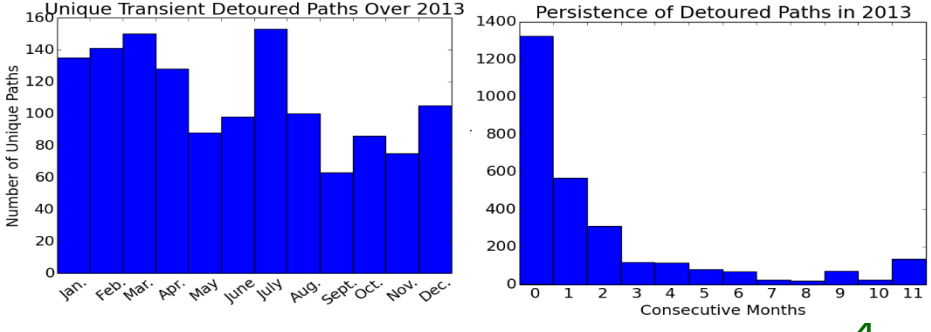
BGP Still Insecure

- Despite years of effort and $$ BGP security is still unsolved
  - Prefix hijacks
  - Routing outages
  - MIM attacks
- If we can't secure it, let's at least monitor it. But:
  - Need many eyes to cover the entire Internet
  - Many eyes generate a lot of data!
  - We must collect and process the data and extract interesting events
  - We must learn to recognize interesting events!
  - We must notify interested parties of those events in a timely fashion

Is this a Real Threat?

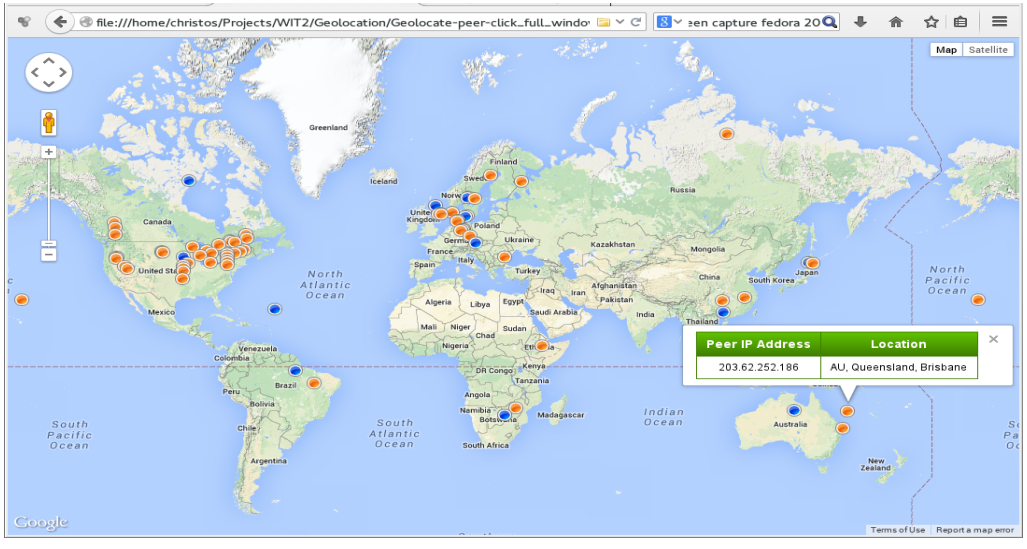
- Prefix Hijacks
  - YouTube hijack and many more
- Outages
  - 2012 Australia outage, Egypt, Syria..
- Detours
  - 2013 Denver - Iceland – Denver
  - who is looking?

http://research.dyn.com/2013/11/mitm-internet-hijacking/



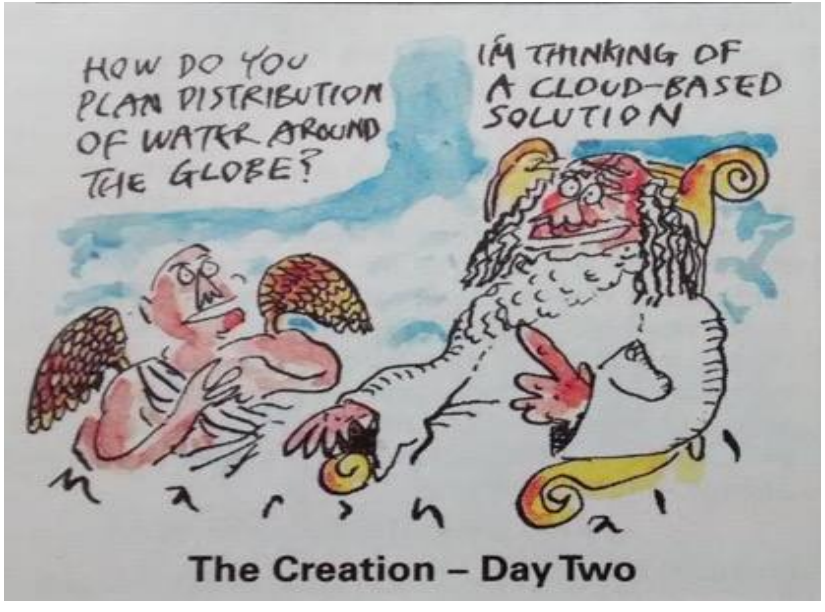
Approach: RouteViews + BGPmon

- Global, real-time BGP monitoring by an ever-expanding collection of eyes
  - ~500 IPv4+IPv6 eyes
  - Simple, file-based archive + xml streaming
- Original BGPMon got the architecture right, but 10-year old custom software hit scaling wall

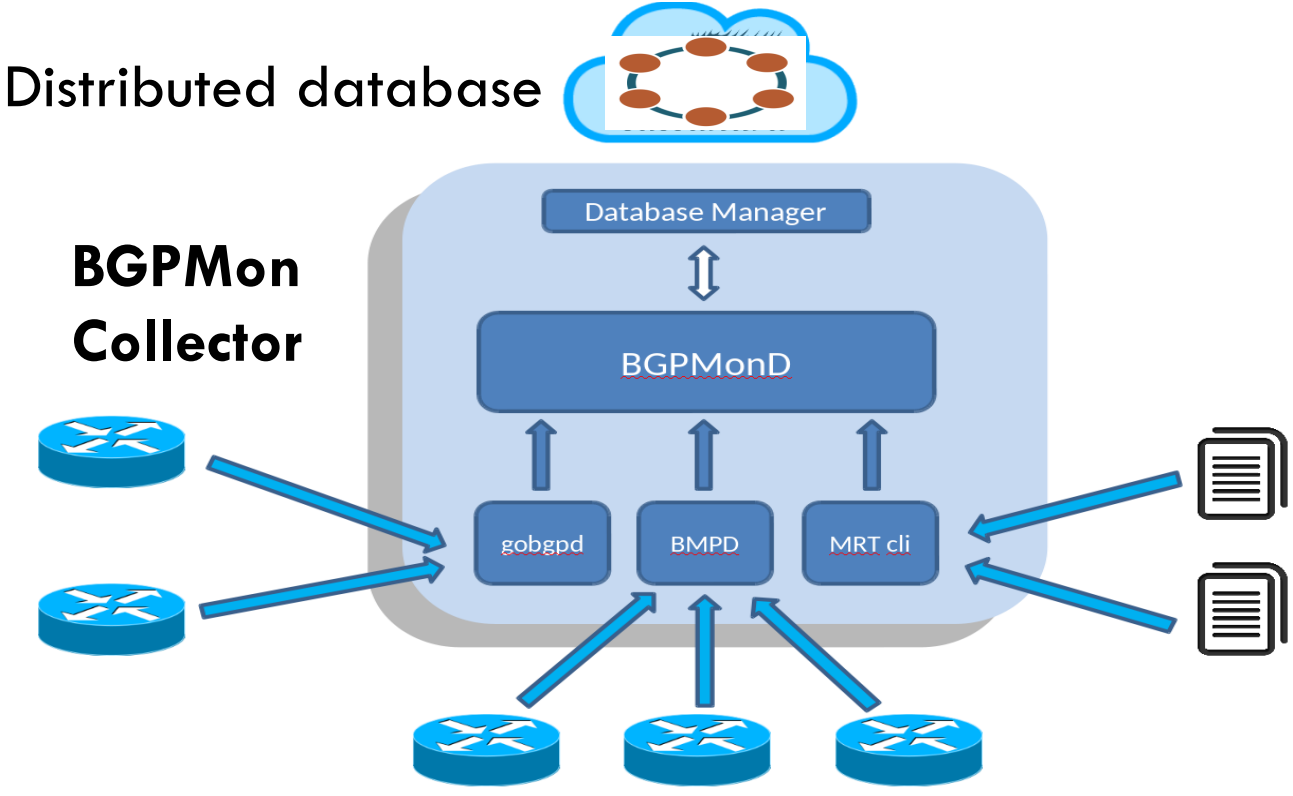


Modernizing BGPMon

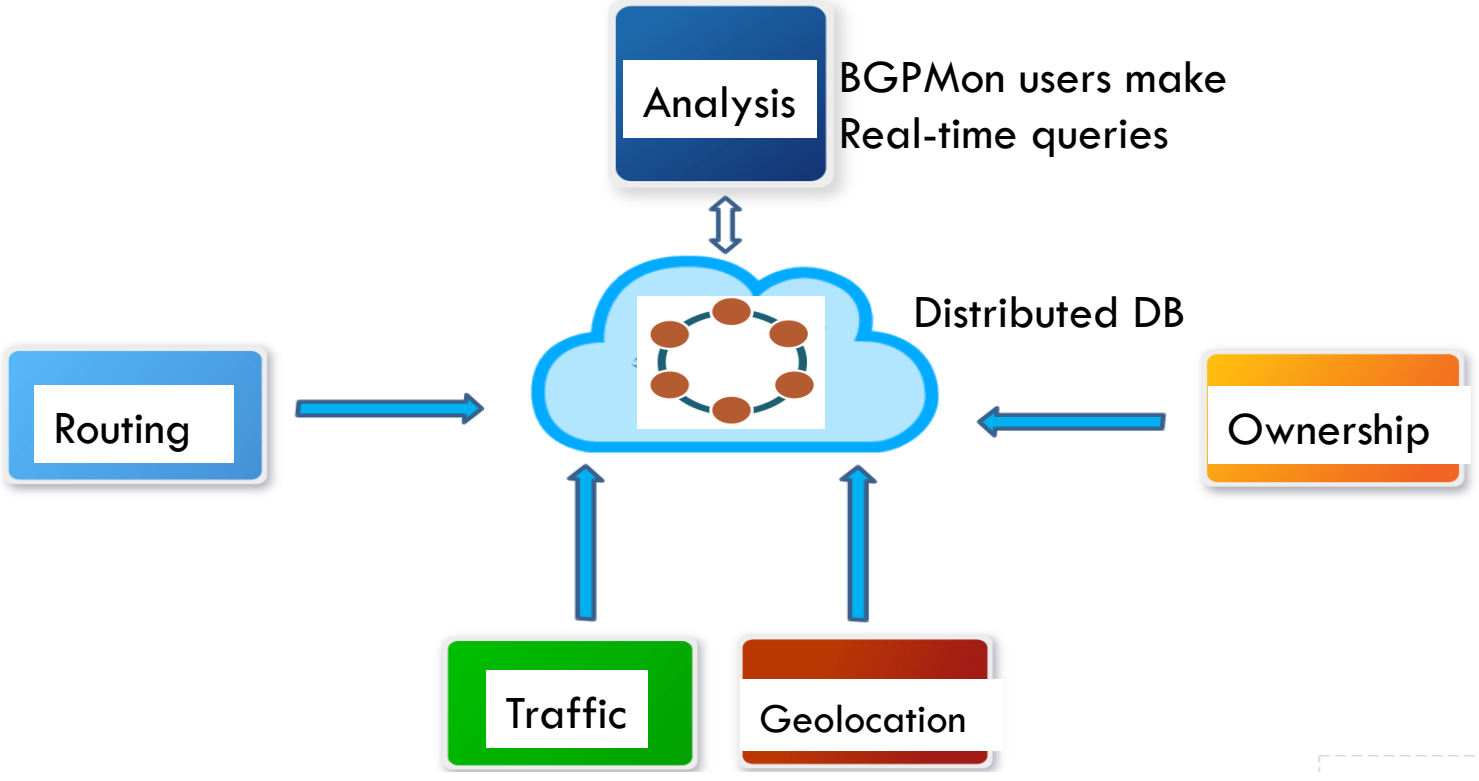
- Goals:
  - Expand capacity, improve robustness, modernize user interface
  - Richer information
  - Private use
  - Geography
- Approach:
  - Enable BGPMon to pair with a cloud based, distributed database
  - Leverage the power of community software
  - Geolocate the eyes, routing prefixes and Autonomous Systems



The New BGPMon.io Collector



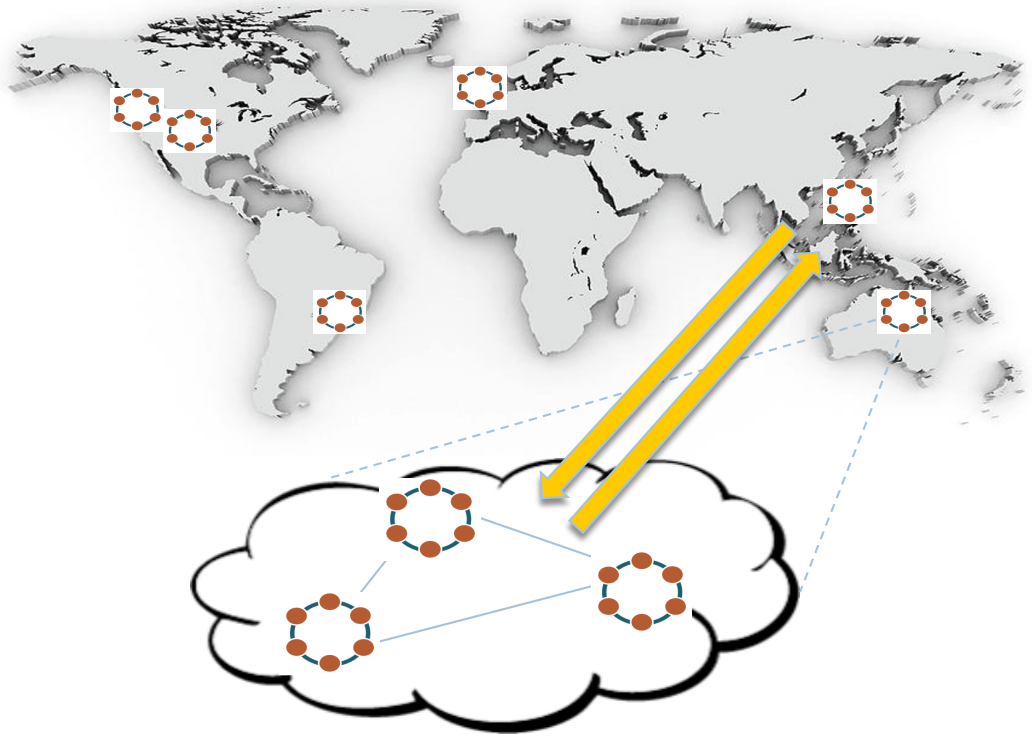
BGPMon.io Data Flow



Planned BGPMon.io Public Deployment

BGPMon.io Private Deployment

- Networks may deploy private instances of BGPMon
  - Monitor classified infrastructure
- Interconnection options with public BGPMon:
  - None
  - Import only
  - Import/Export



New Service: BGPMon Archive

- Web-based archive with time-based BGP data retrieval
- Contains **all data** from RouteViews and Colorado State U collectors
- BGP update messages & RIBs, in MRT, JSON and protobuf format
- Enables continuous pull of data with option to receive only new updates since the previous request
- **Works now, try it:** http://bgpmon.io/archive/help

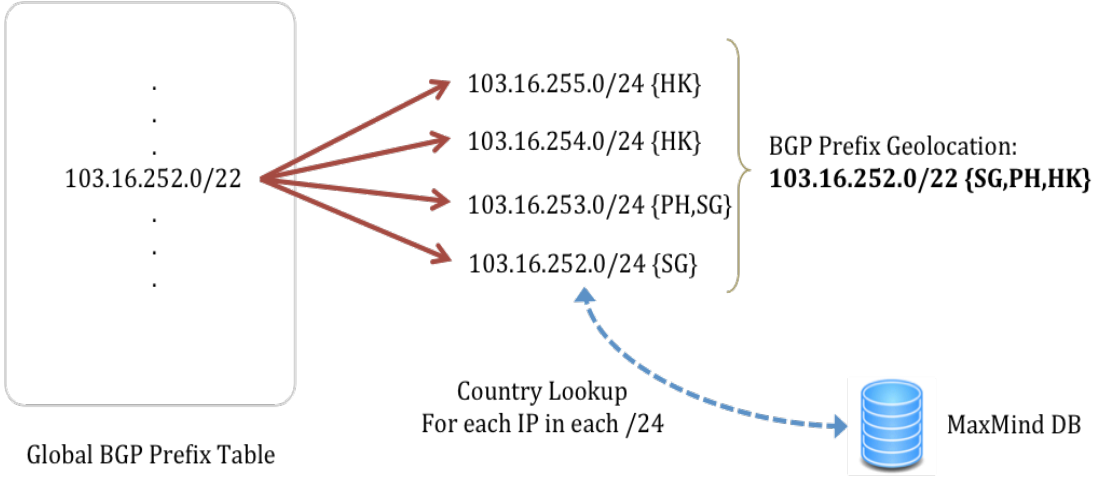
Protobuf Backend Benefits

- Direct interface into BGP data
- Data in Protocol Buffer Record Store
- New library: *protoparse to* turn BGP messages -> protobufs
- We parse natively most of BGP spec
- We produce "record" files with 30% size reduction compared to original MRT
- On-the-fly marshaling into JSON and XML through golang standard library
- **Works now, try it:** http://bgpmon.io/archive/help

New Service: AS/Prefix Geolocation

- Determine the **country** an AS or a prefix geolocates
- Static databases not reliable, they quickly go out of date
- Better approach: periodic geolocation (monthly) based on observed BGP activity and current geolocation databases
  - Simple lookup function: given prefix or AS and a month, return country (or countries)
  - Dynamic service can track the IP marketplace (address geographical movement) and take advantage of improvements in IP geolocation DBs
  - Dynamic service can provide historical record of prefix ownership and geography
- Works now, try it: http://geoinfo.bgpmon.io/

Geolocating Prefixes/ASes



- To geolocate a BGP prefix we first geolocate all constituent /24s using Maxmind by looking up all IP addresses
- Prefix country geolocation is the set of resulting countries
- AS country geolocation is the set of resulting countries from all the prefixes the AS advertises

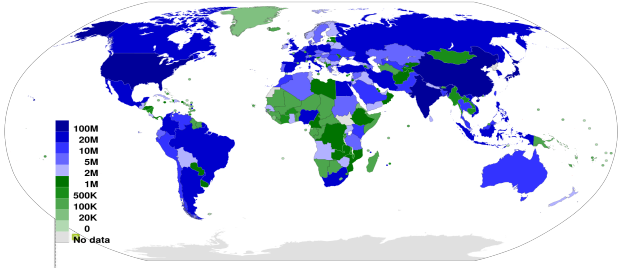
Application: International Detours

- An international *detour*: A path that originates in one country, crosses international boundaries and returns back to the origin country
- Leverages country-level geolocation of prefixes and Autonomous Systems

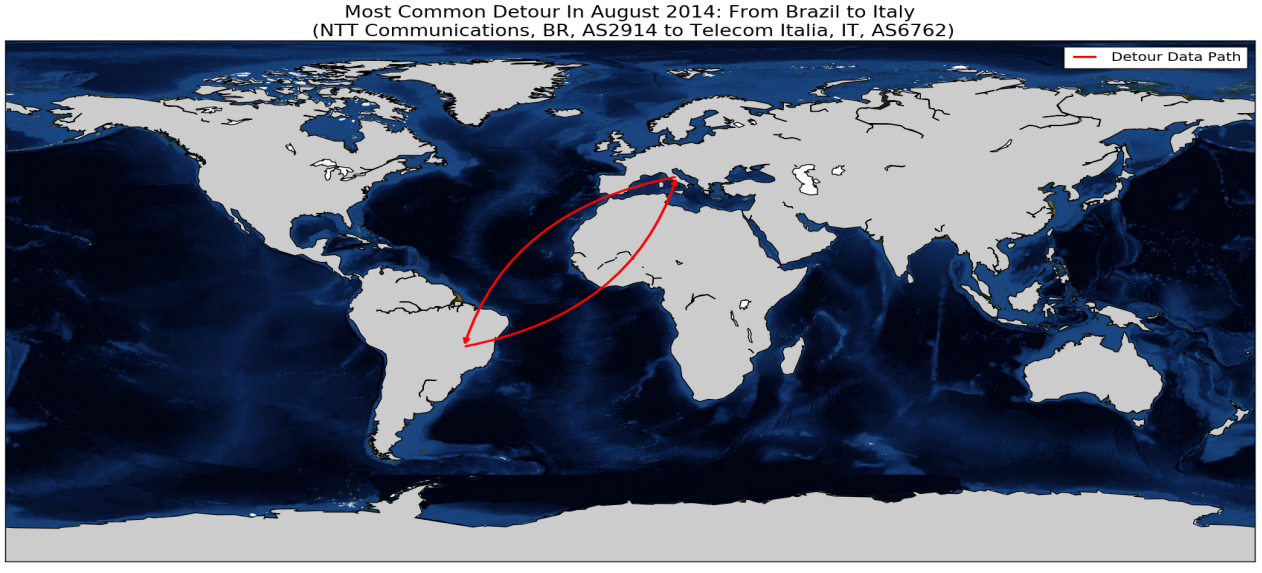
Why Detect International Detours?

Detours can help:

- locate areas of sparse network presence – may point to business opportunities
- comply with regulatory requirements
- detect network problems
- assess traffic sniffing potential



Example: A Persistent Detour

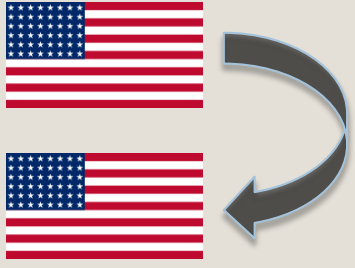


Top Detour Origin ASN	Most Common Detour Destination	Total Percentage	Percentage of detours that went to most common destination
2914 (NTT-COMMUNICATIONS) (BR)	6762 (TELECOM ITALIA) (PE, DZ, AR, EU, GR, US, IT, EG)	14.08%	73.70%

Example: A Transient Detour

- A ***transient*** detour we detected in August 2014:

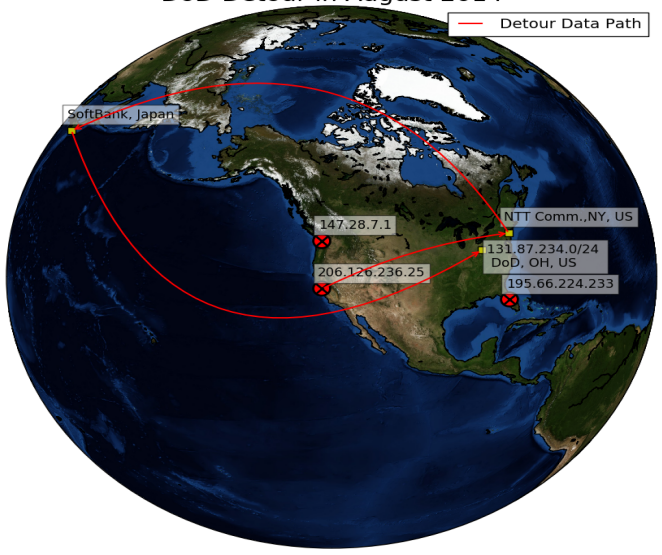
AS Path seen at Client in US:
19151 174 2914 17676 209 721
27066 27046



AS17676
SoftBank, Japan

131.87.234.0/24
US Department Of Defense
AS27046

DoD Detour in August 2014



- 3 distinct RouteViews peers saw this detour a total of 13 times
  - Detour lasted as little as 6 hours and as long as 48 hours

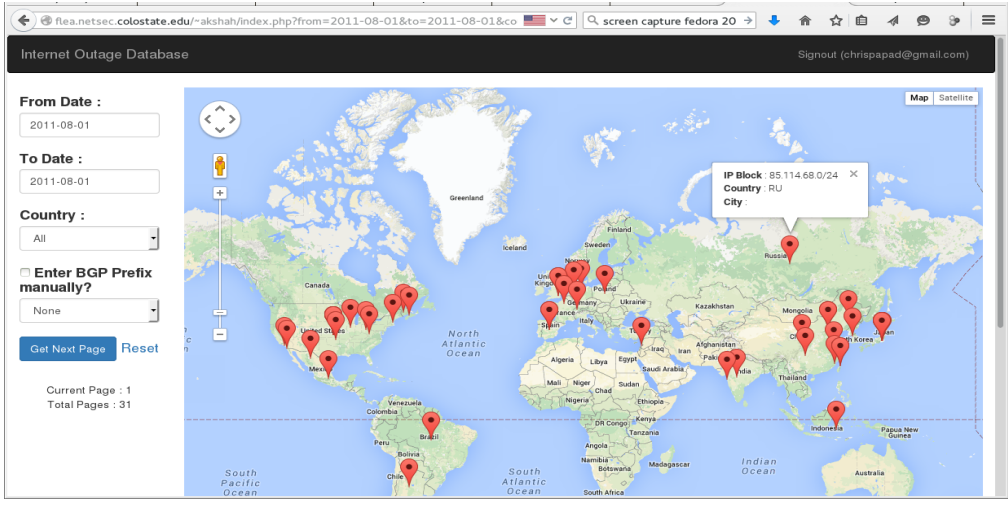
Transient detour: Detour that is seen in RIBS for less than 72 hours

New Service: BGP Hijacks

- Currently in beta testing with Charter and Comcast
- Process:
  - You give us your ASNs
  - We determine all the prefixes you advertise (and find some additional ASNs along the way) from the live BGP feed
  - We start monitoring, learn your peers/customers to avoid false positives
  - Report potential hijacks to you
- Avoiding false positives is the hardest problem
  - Evolving process using historical data, peering data and info from you
- Contact us if you want to join the fun!

Coming Soon: Data Plane Outages

- Everyone cares about outages!
- Outages may be visible at the control plane, data plane or both
- BGPMon can see control plane outages
- Working to ingest data plane outages from ISI's LACREND



Conclusions

- BGPMon.io is a clean slate implementation of old BGPMon
- Strong focus on serving the community
- New interface and services: archive, protobuf interface, AS/prefix country geolocation, hijacks and outages
- BGPMon.io offers multiple new interfaces to satisfy different applications
- We invite everyone to try BGPMon.io (governments, federal agencies, companies)
- We need your feedback! Don't be shy!

Contact Information

Spiros Thanasoulas
Colorado State University
dsp@colostate.edu
+1-970-491-7015

Christos Papadopoulos
Colorado State University
christos@colostate.edu
+1-970-491-3267

To peer with BGPmon and for more information: www.bgpmon.io