Bigfoot: A Geo-based Visualization Methodology for Detecting BGP Threats

Meenakshi Syamkumar*, Ramakrishnan Durairajan*, Paul Barford*+

*University of Wisconsin-Madison

+comScore, Inc.

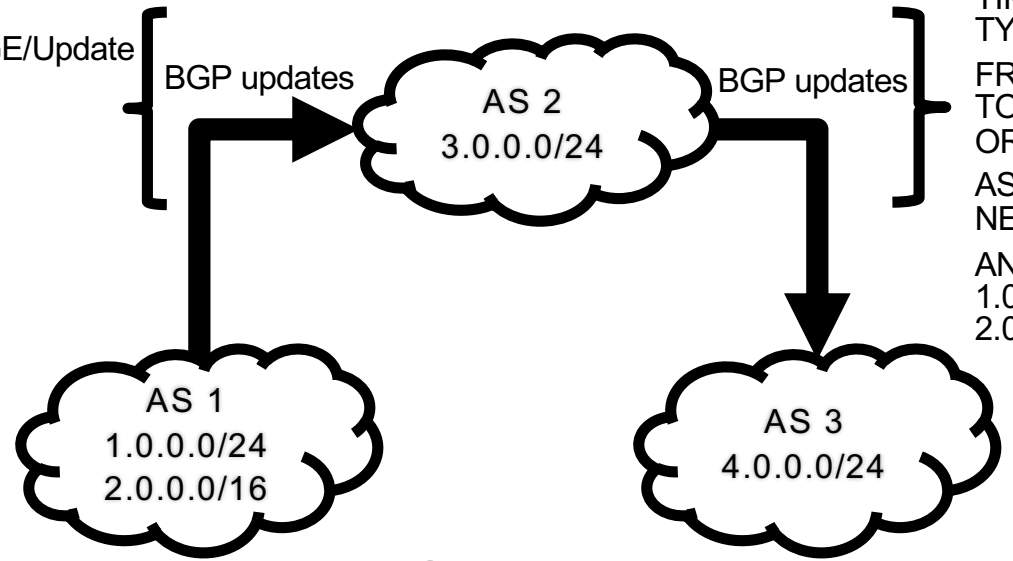
Motivation

- Enormous volume and diversity of BGP updates present challenges in network operations and detecting unwanted behavior
- Graphical visualization is a well known method for assessing complex datasets
- Prior visualization methods for BGP focus on AS topologies identified through AS path structure
- Bigfoot's goals:
  - Can consistent visualizations be created to represent geographic footprint of network prefixes?
  - Can such visualizations be used in detecting security threats like prefix hijacks, man-in-the-middle attacks?

Primer on BGP

- BGP enables transmission of reachability information between Autonomous Systems (AS)

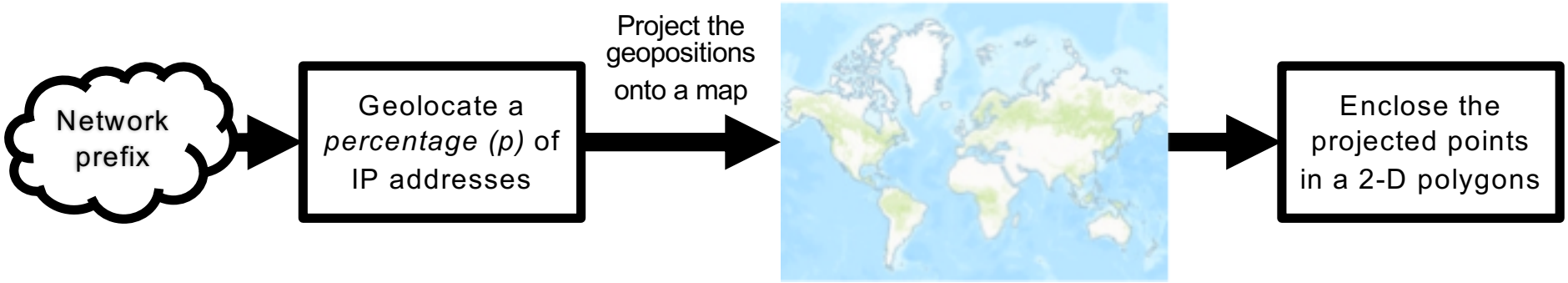
TIME: 10/01/16 00:00:00
TYPE: BGP4MP/MESSAGE/Update
FROM: 2.0.0.100 AS1
TO: 3.0.0.101 AS2
ORIGIN: IGP
ASPATH: 1
NEXT_HOP: 2.0.0.100
ANNOUNCE
1.0.0.0/24
2.0.0.0/16



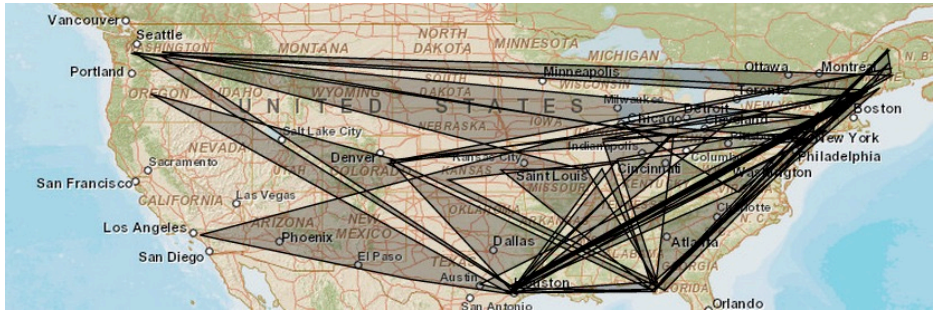
TIME: 10/01/16 00:01:00
TYPE: BGP4MP/MESSAGE/Update
FROM: 3.0.0.101 AS2
TO: 4.0.0.102 AS3
ORIGIN: IGP
ASPATH: 2 1
NEXT_HOP: 3.0.0.101
ANNOUNCE
1.0.0.0/24
2.0.0.0/16

Network footprint visualization

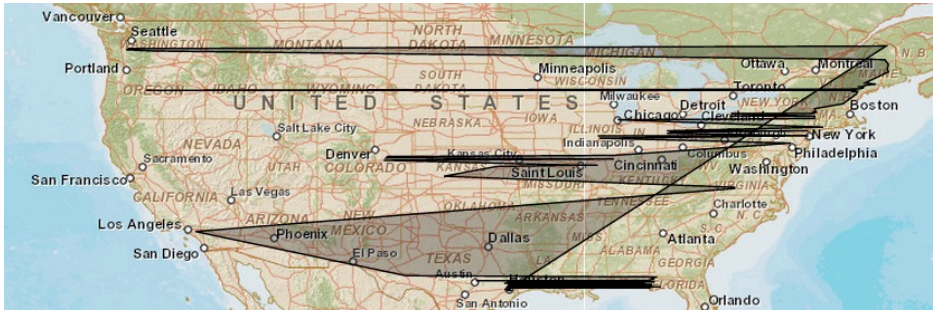
- Geolocation has always been associated with individual IP addresses
- Can we obtain meaningful visualizations by considering geo-footprint of the entire network prefix?



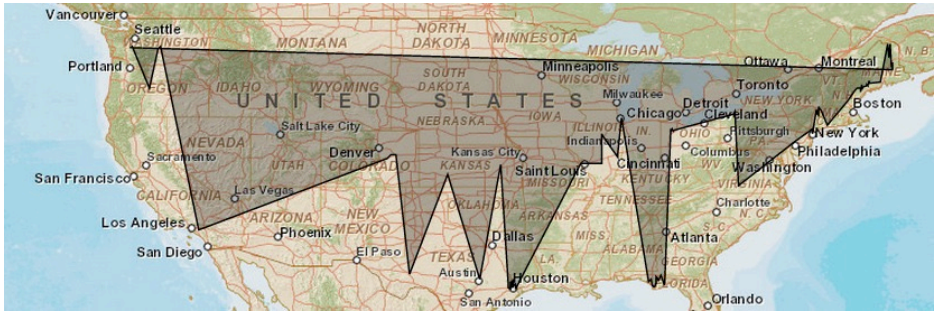
Naïve network footprint visualizations



Unsorted



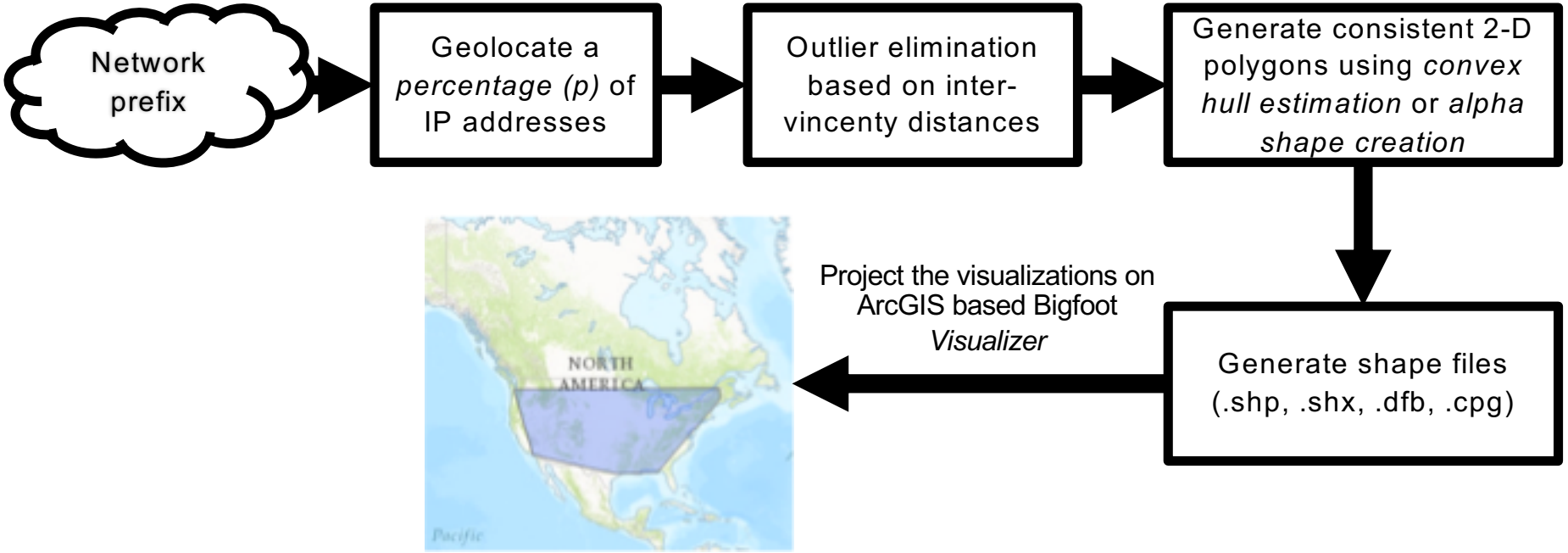
Latitude-sorted



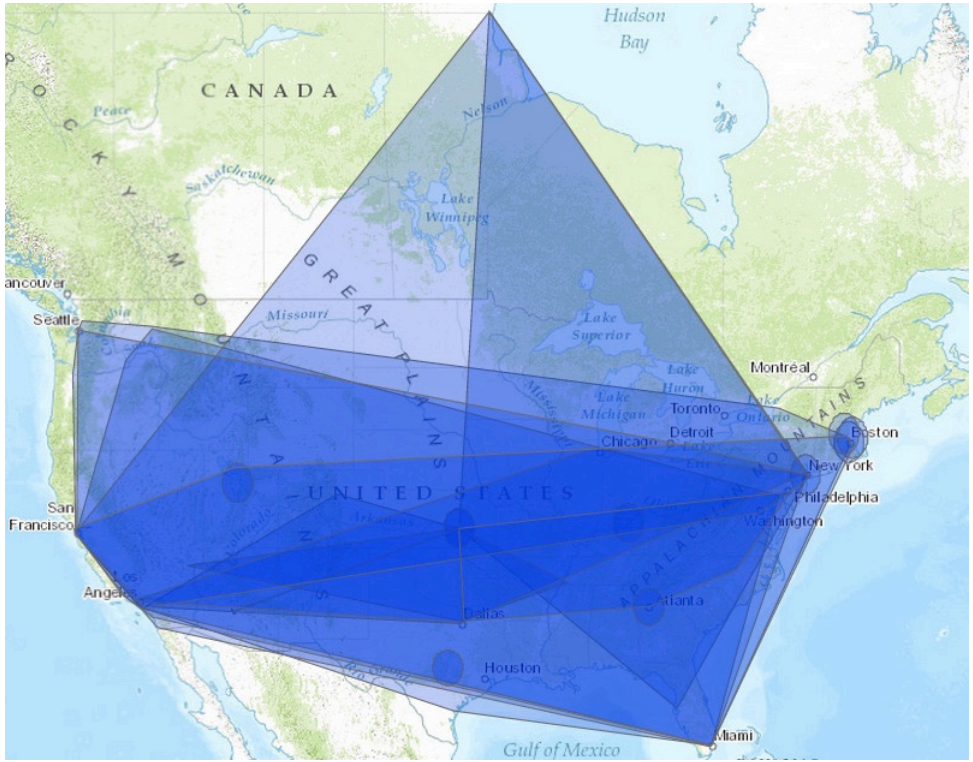
Longitude-sorted

Footprint of Fairpoint Communications (AS 32645, 216.227.0.0/16)

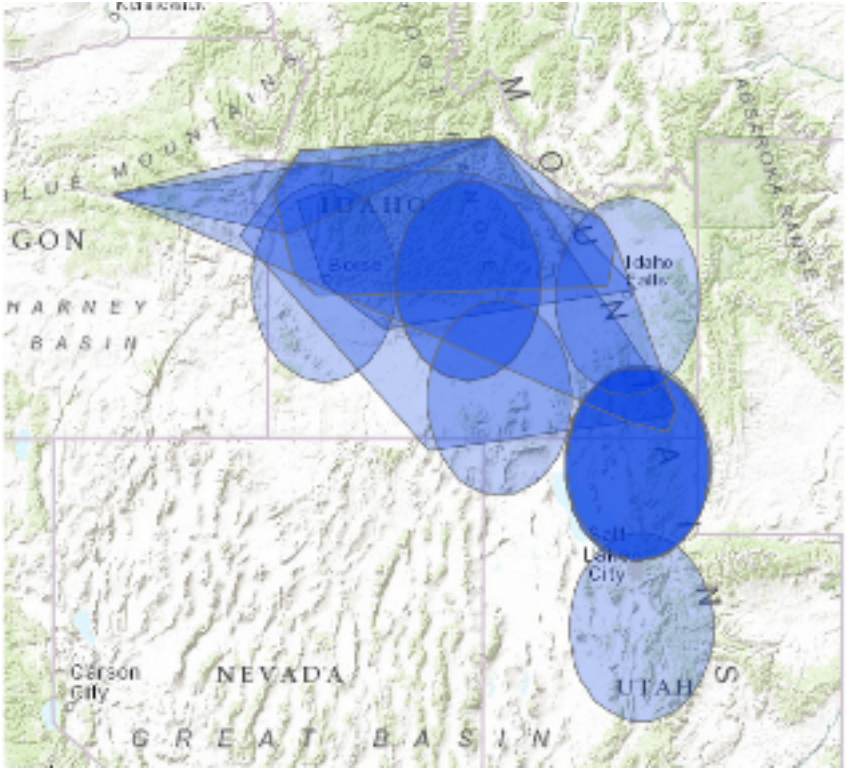
Bigfoot methodology



Bigfoot visualizations



Footprints of AS2828 and AS7014
XO Communications



Footprint of AS15305
Syringa Networks

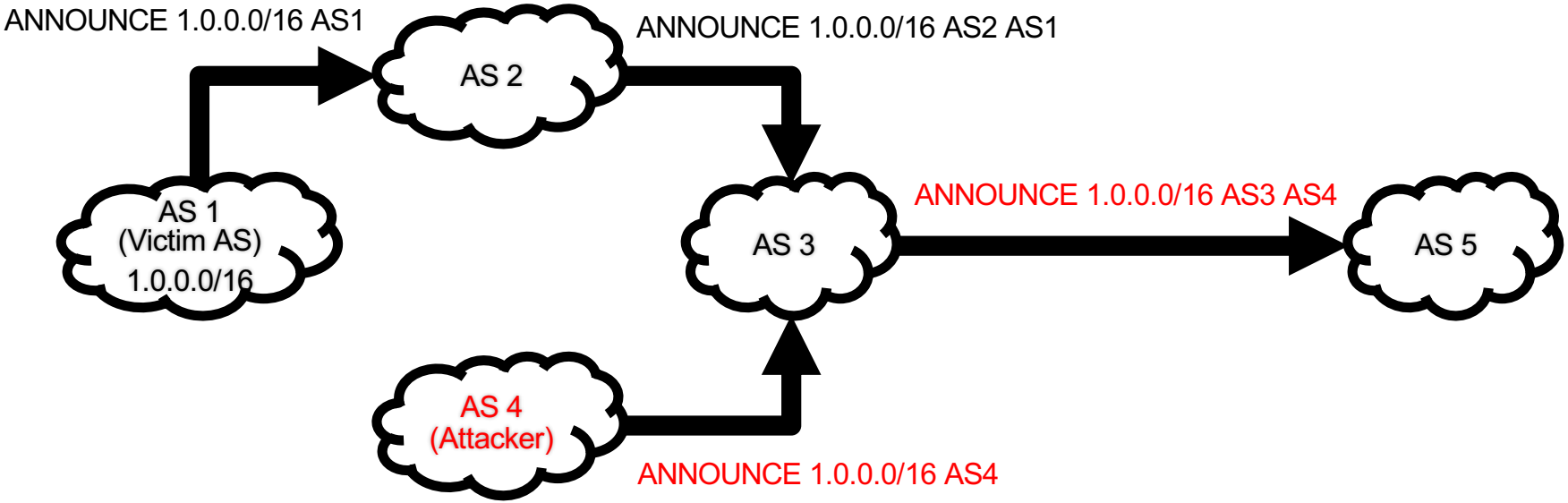
ms@cs.wisc.edu

BGP security threats

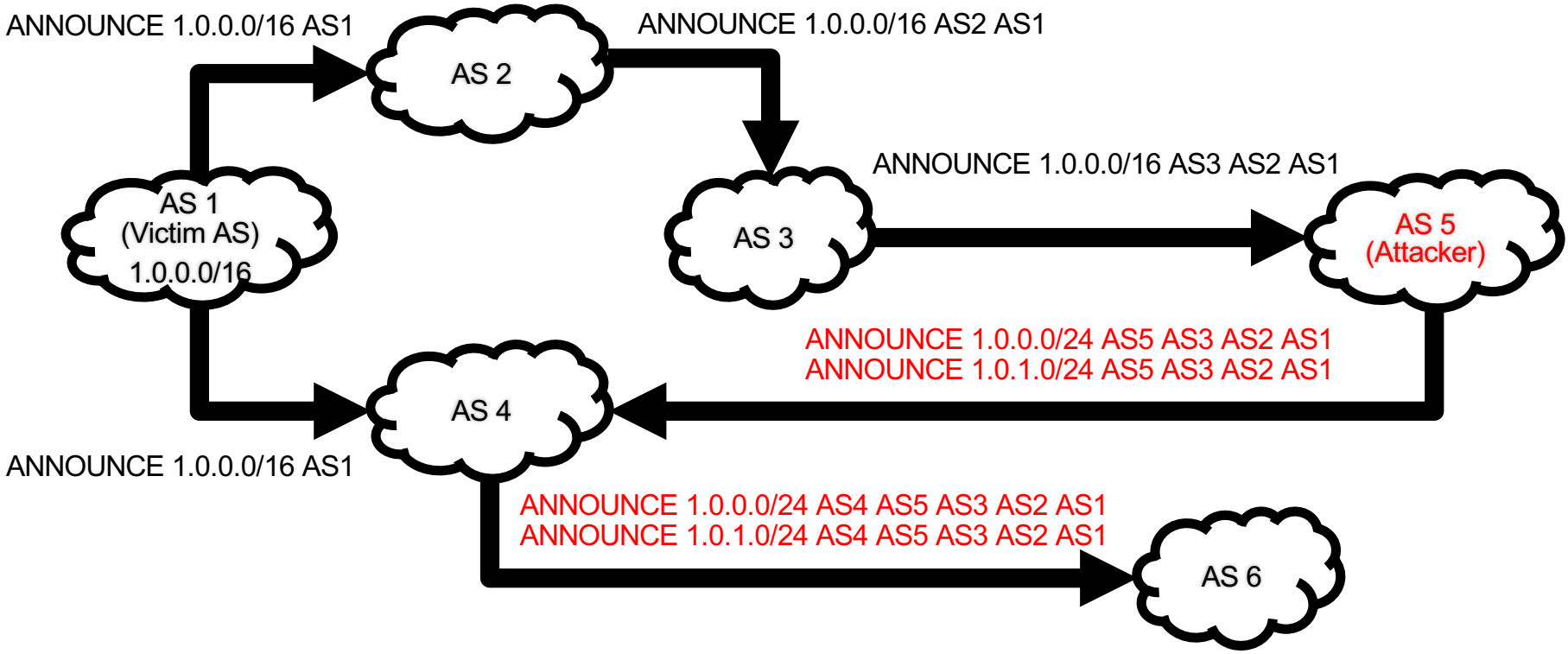
BGP is susceptible to misconfigurations and malicious attacks like:

- Multiple Origin AS (MOAS) conflict [Zhao *et al.*, ACM SIGCOMM Workshop on Internet Measurement, 2001]
- Man-in-the-middle attack [Ornaghi *et al*., Blackhat Conference, 2003]
- Routing leak [Mahajan *et al.,* ACM SIGCOMM Computer Communication Review, 2002]
- De-Aggregation attacks [Nordström *et al*., ACM SIGCOMM Computer Communication Review, 2004]
- Contradictory advertisements [Nordström *et al*., ACM SIGCOMM Computer Communication Review, 2004]
- Origin and export misconfigurations [Mahajan *et al.,* ACM SIGCOMM Computer Communication Review, 2002]

BGP MOAS conflict



BGP man-in-the-middle attacks



Bigfoot anomaly detector

- Select a “timeOfInterest” for anomaly detection in BGP update stream.
- Establish baseline for “normal” behavior:
  - Select updates from previous “k” days
  - Aggregate announced subnets based on “ASPATH”
  - Generate the Bigfoot visualizations for the networks
- For every update in the “timeOfInterest” determine anomaly based on thresholding
- Thresholding is done by performing:
  - Comparison operations on the polygons - equals and/or contains comparisons
  - Comparison of number of polygons, area of polygons
  - Comparison of the geographic coverage of the polygons

Bigfoot anomaly detector

For every update in the “timeOfInterest” determine anomaly based on thresholding:

- Compare “ASPATH” with baseline information and if the “ASPATH” is previously observed path:
  - Generate the polygons for the networks in current update
  - Perform comparison operations with threshold as “perfect mismatch”
  - On mismatch, “Prefix2AS” dataset is looked up to filter network expansion related changes
  - Rest of the networks are classified as victims of attacks
- If the “ASPATH” is previously unobserved path:
  - Identify the closest matching “ASPATH”
  - Perform comparison operations with threshold as “perfect match”
  - Matched polygons correspond to networks that are victims of hijack

Bigfoot evaluation

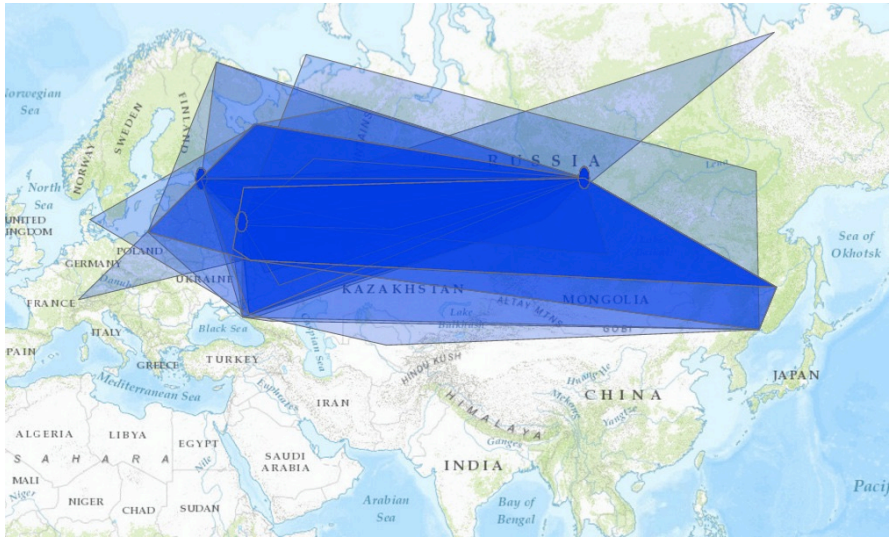
BGP archive datasets evaluated:

- February 2013 to July 2013 (D1)
- January 2015 to June 2015 (D2)

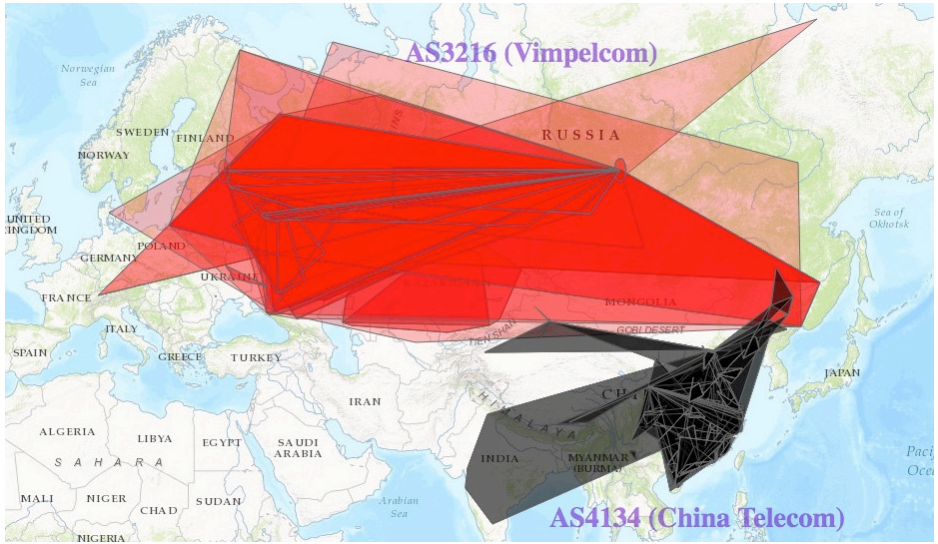
Candidate anomalous events detected:

- In D1: 73 events
- In D2: 66 events

Applications of Bigfoot: BGP routing leak attack



Normal routes from Vimpelcom (AS3216)



China Telecom (AS4134) leaked several routes from Vimpelcom (AS3216)

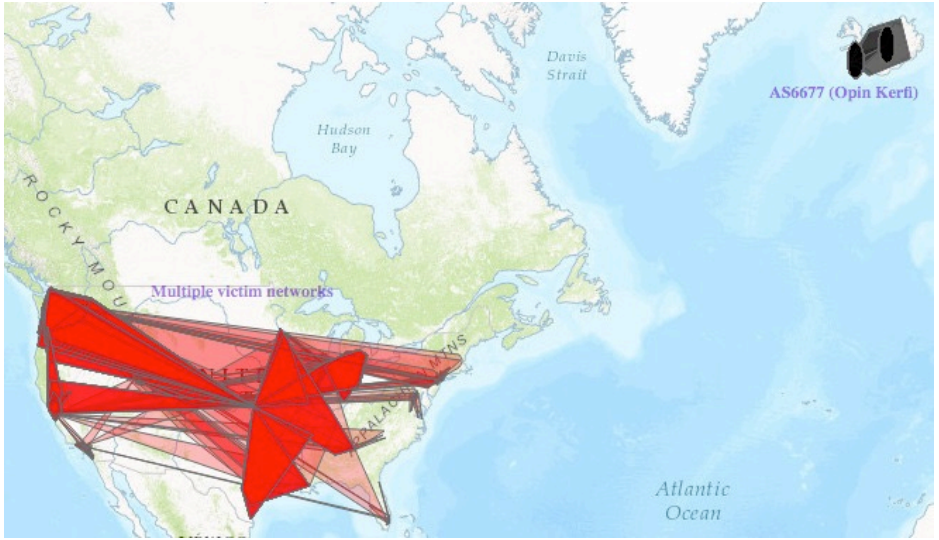
Applications of Bigfoot: BGP redirection attack

Normal operations of victim networks

Belarusian ISP GlobalOneBel (AS28849) hijacked traffic from multiple networks

Applications of Bigfoot: BGP man-in-the-middle attack

Normal operations of victim networks



Icelandic provider Opin Kerfi's ISP Síminn (AS 6677) hijacked traffic from multiple networks

Classification using meta-information

Three classes based on the types of anomalies:

- C1A: the hijacking AS inserts itself or replaces one or more of the ASes in the AS path
- C1B: the prefixes announced in the update forms an entirely new AS path
- C1C: the prefixes announced in the update belongs to a different address registry

$C1_A$		$C1_B$		$C1_C$	
D1	D2	D1	D2	D1	D2
25	23	44	41	9	7

Classification using geography

Three classes based on the extent of geographic impact:

- C2A: anomalies distributed across different continents
- C2B: anomalies spread across different countries, but within the same continent
- C2C: regional anomalies where the prefixes get geolocated to different regions in the same country.

$C2_A$		$C2_B$		$C2_C$	
D1	D2	D1	D2	D1	D2
36	26	31	37	6	3

Conclusions

- Convex hulls and alpha shapes enable creation of consistent visualizations for network footprint
- Bigfoot's visualizations enable identification of key operational events in large volume BGP datasets
- Future work:
  - Expand Bigfoot's applicability to broader security scenarios and operational misconfigurations
  - Analyzing the potential of network footprint visualization in network planning and risk assessment
  - Reach out to network operators to validate the events which lack ground truth information
  - Analysing the variation of percentage of IP addresses geolocated for the visualizations

Bigfoot is available as part of Internet Atlas (http://internetatlas.org/)

Questions?