A Measurement Study on BGP AS Path Looping (BAPL) Behavior

Shenglin Zhang Ying Liu Dan Pei

Tsinghua University

Outline

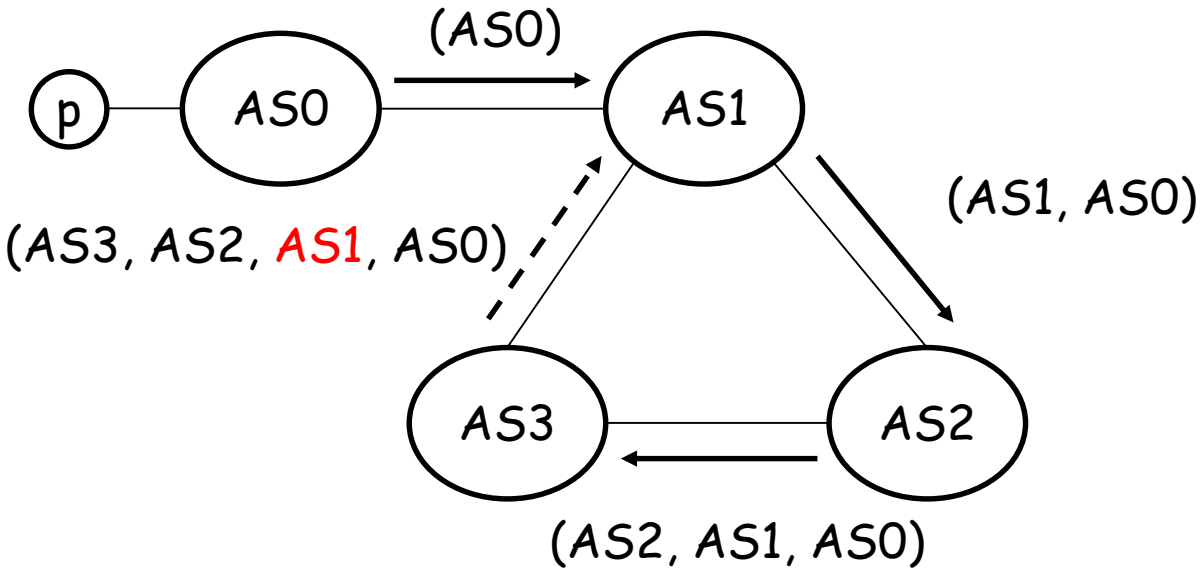
- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

Outline

- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

Background

BGP is supposed to eliminate path looping.



Background

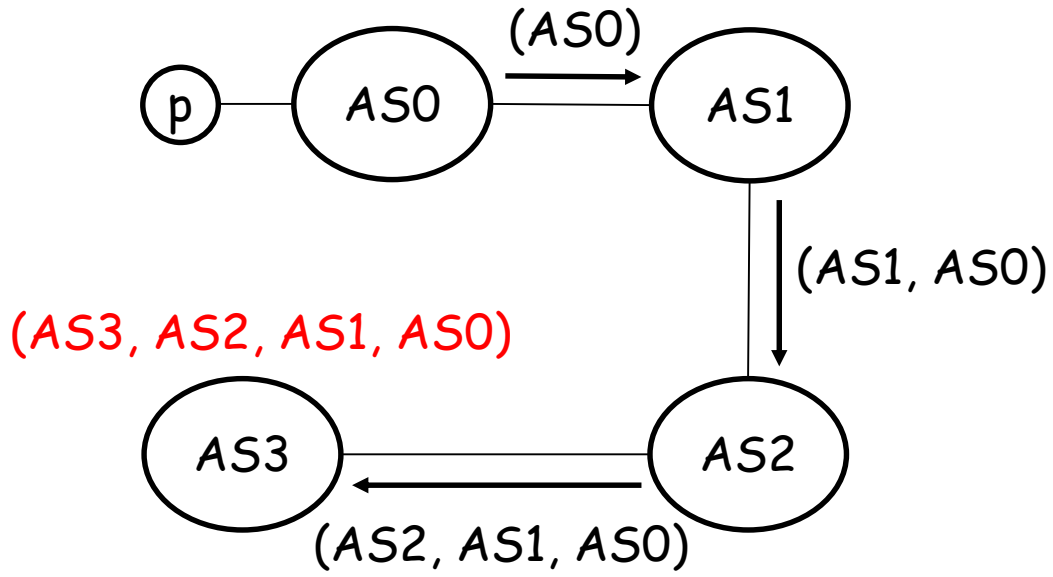
- A BGP AS path looping (BAPL) occurs if there is a loop in the AS-PATH attribute.
- Previous research has shown the evidence of BAPL(SIGCOMM 02, IMC 12).
- BAPL has not been systematically studied.

Outline

- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

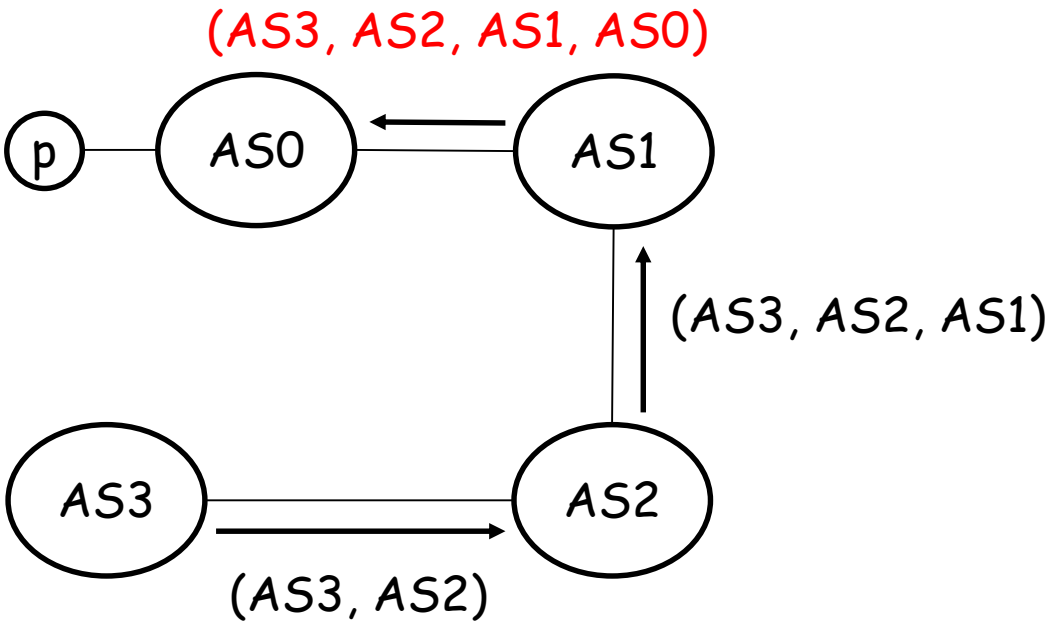
The BGP AS path and the forwarding AS path

The BGP AS path denotes the list of ASes through which the BGP update messages propagate.



The BGP AS path and the forwarding AS path

The forwarding AS path is the list of ASes that actually forward the data packets.



The BGP AS path and the forwarding AS path

- They are not always identical
  - aggregation/filtering
  - forwarding anomalies
- Traceroute is employed to collect the forwarding AS paths.
- Forwarding AS path loop is attributed to BAPL
  - The forwarding AS path loop is identical to the BGP AS path loop

Datasets of BGP AS path

- Oregon RouteViews route-views4
- BGP routing table (RIB) : every two hours
- BGP routing updates: every 15 minutes
- Attributes: timestamp, peer IP, peer AS, prefix, AS-PATH, origin AS.
- Collect the RIB data at 01/01/2010 00:00:00
- Collect BGP update data in 1456 days from 01/01/2010 to 12/31/2013.

Outline

- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

Will BAPL lead to forwarding loops

On 09/08/2013, a BAPL (AS1299, AS6453, AS577, AS7788, AS6407, AS7788) is observed.

- Destined for prefix 64.26.148.0/24
- Monitor 80.91.255.62 (from AS1299)
- Lasted more than a few days

The traceroute resulted from 80.91.255.62 to 64.26.148.28 witnessed a forwarding loop.

Hop	Router address	AS number
1	213.155.133.147	1299
2	213.155.133.142	1299
3	213.155.130.51	1299
4	80.91.249.29	1299
5	213.155.131.139	1299
6	213.248.100.178	1299
7	63.243.128.42	6453
8	64.86.85.1	6453
9	216.6.87.9	6453
10	216.6.98.58	6453
11	64.86.85.1	6453
12	216.6.98.58	6453
13	67.69.218.3	577
14	*209.217.64.37*	*7788*
15	*206.191.0.89*	*7788*
16	*67.230.128.70*	*6407*
17	*209.217.64.37*	*7788*
18	*206.191.0.89*	*7788*
19	*67.230.128.70*	*6407*
20	*209.217.64.37*	*7788*
21	*206.191.0.89*	*7788*
22	*67.230.128.70*	*6407*
...	...	...

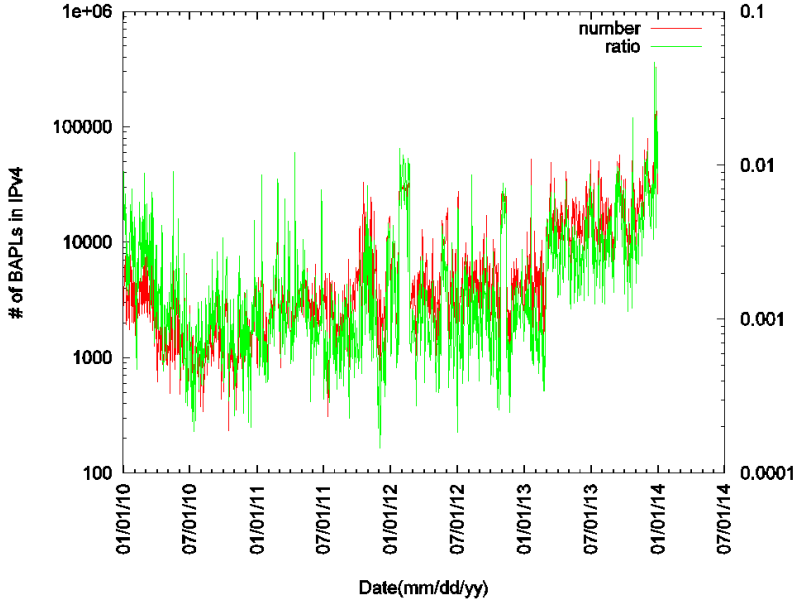
Will BAPL lead to forwarding loops

- Only 1% of the BGP AS path loops accounted for forwarding loops.
- This percentage might be biased
  - We only sampled the signaling AS path loops which we could use looking glass to run traceroute.
- Motivates us to carry out more in-depth researches on BAPL behavior.

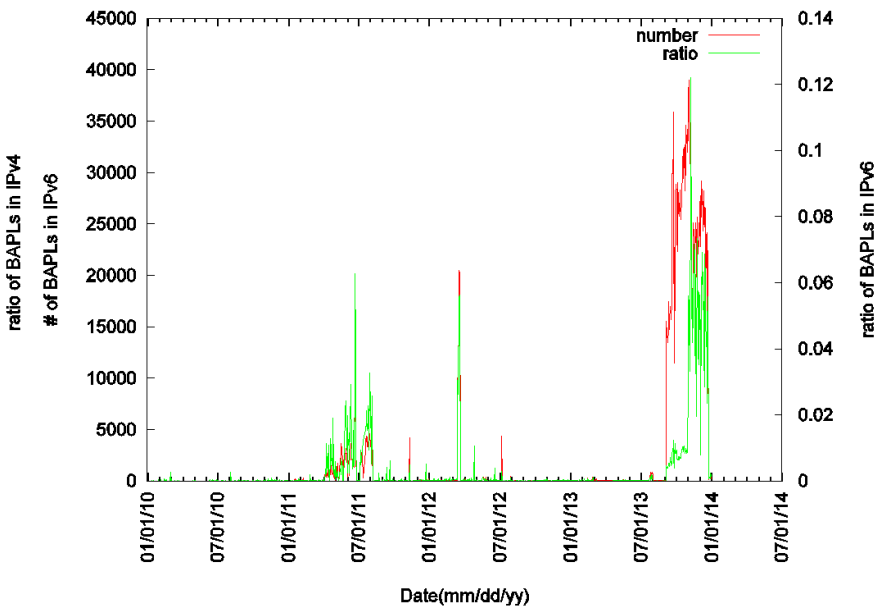
Outline

- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

Total number and ratio of BAPLs



The number and ratio of BAPLs in IPv4



The number and ratio of BAPLs in IPv6

- More than 8000 BAPL updates for IPv4 per day on average.
- More than 2000 for IPv6.

Total number and ratio of BAPLs

Medians of BAPLs per year

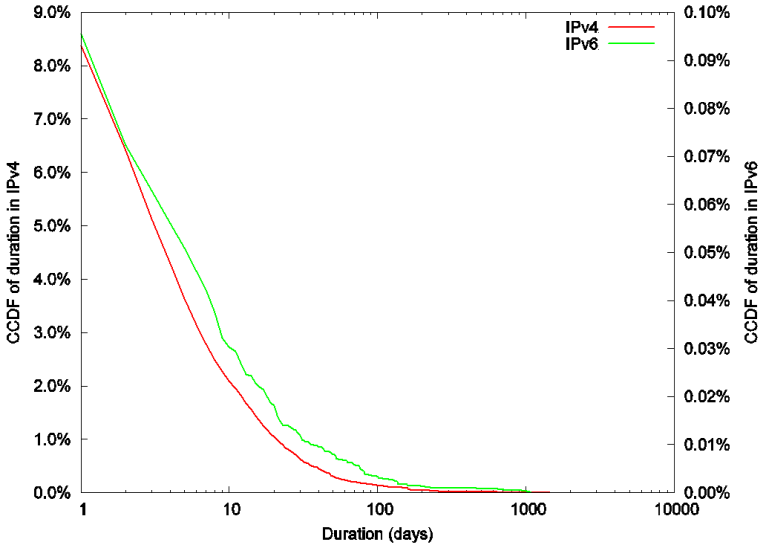
Year	Number of IPv4	Ratio of IPv4	Number of IPv6	Ratio of IPv6
2010	1580	1.03×10^{-3}	0	0
2011	2870.5	9.23×10^{-4}	21.5	7.65×10^{-5}
2012	4603	1.08×10^{-3}	14	5.01×10^{-5}
2013	15808	2.94×10^{-3}	21	5.07×10^{-5}

- In IPv4, the number of BAPLs increased dramatically from 2010 to 2013.
- Due to the explosion of global BGP routing table, the ratio of BAPLs kept stable in 2011 and 2012.
- In IPv6, the number of BAPLs increased in 2011, decreased in 2012, and stayed stable in 2013, so as the ratio.

Outline

- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

Duration of BAPLs



The CCDFs of the distribution of duration for BAPLs

- More than 91% of the loops lasted shorter than one day.
- Non-trivial number of BAPL updates lasted longer than a month.

Duration of BAPLs

Average BAPL duration

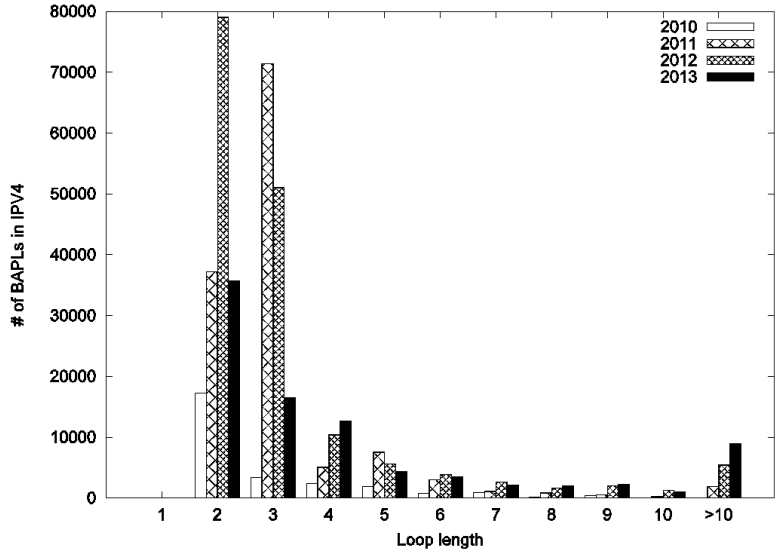
Measured data set	Averages in IPv4(days)	Averages in IPv6(days)
Longer than 0 day	9.91	4.72
Longer than 1 days	13.11	23.41
Longer than 9 days	37.70	60.97
Longer than 29 days	87.89	131.26
Longer than 89 days	224.76	322.11

- Excluding the BAPLs that last shorter than 1 day, the average duration is 13.11 days in IPv4 and 23.41 days in IPv6.
- The long lasting BAPLs can not be explained by misconfigurations.

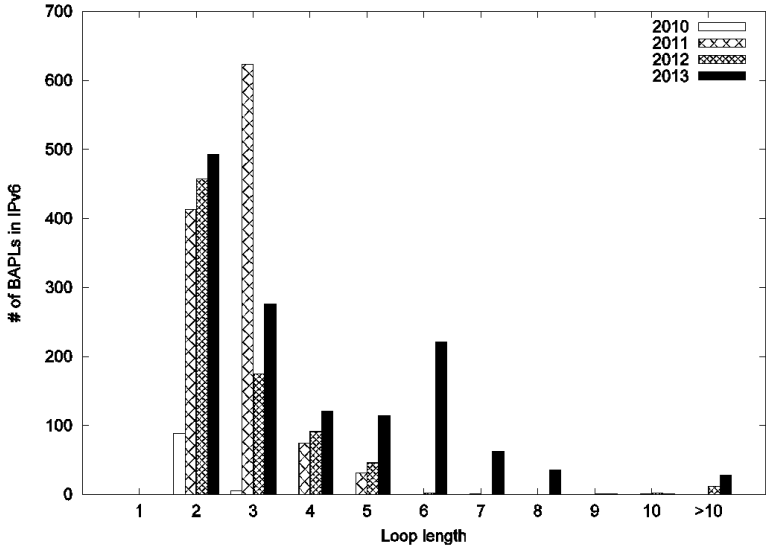
Outline

- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

Loop length of BAPLs



Loop length of BAPL in IPv4



Loop length of BAPL in IPv6

- Most of BAPLs have a 2-hop or 3-hop loop.
- It is easy to amplify the amount of traffic remarkably in the links that appear in the loops.

Outline

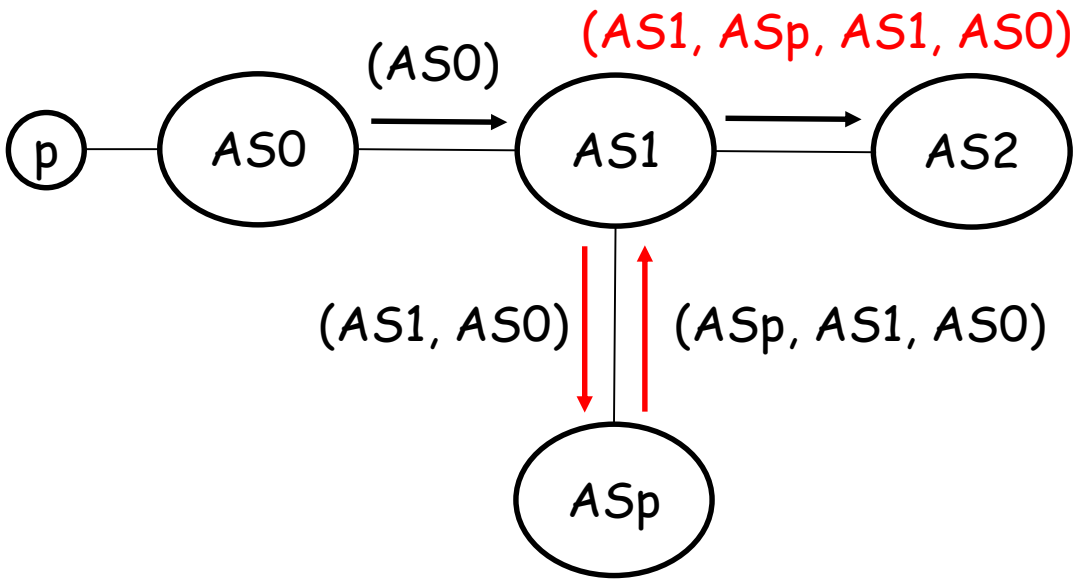
- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

Private AS number leaking

- Private AS number
  - When a customer AS communicates with a single provider AS using BGP, private AS number can be used.
  - The routing policy between the provider AS and the customer AS is not visible in the Internet.
  - Private AS number can be leaked to the Internet due to misconfigurations.
- 1.76% of BAPLs are definitely caused by private AS number leaking in IPv4.

Private AS number leaking

An example of why private AS number leaking onto the Internet might lead to BAPL.



Outline

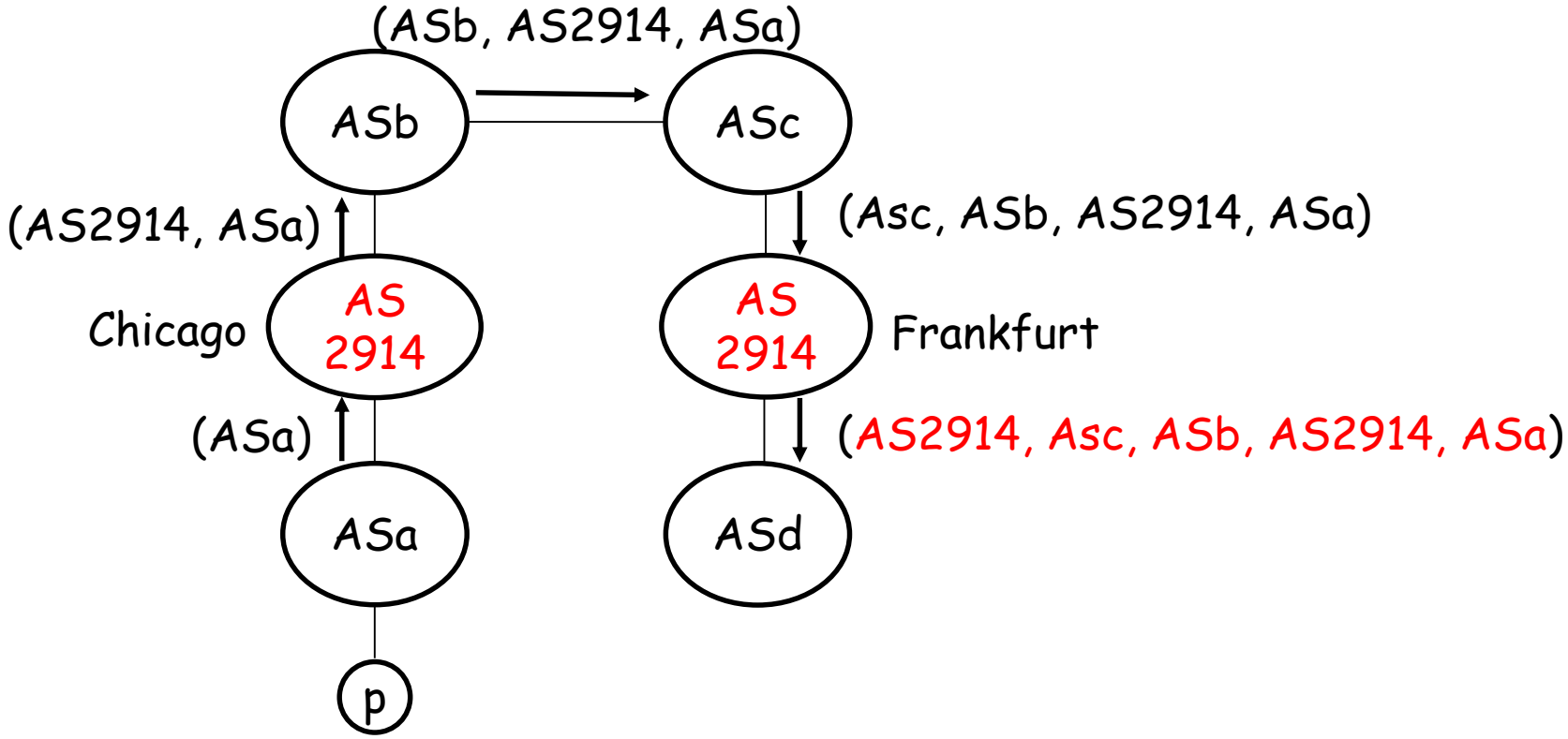
- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

Multinational companies

- Some multinational companies have exchange-points all over the world.
- Several exchange points may share the same AS number a.
- Operators configure their routers to accept routes whose AS-PATH attributes containing Asa.

Multinational companies

An example of why multinational companies might lead to BAPL.



Outline

- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

Preventing particular AS from accepting routes

- Operators of ASa might prepend ASb so that ASb will not pick up the routes from ASa.
- On 08/18/2011, a rerouting experiment which applied to AS47065 is conducted.

- A looped AS path (47065, a, 47065) for prefix 184.164.255.0/24 was announced.
- ASa could not accept this route later.
- Related traffic would not pass through ASa.

Outline

- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

Faulty configurations or malicious attacks

- Argus is an agile system to detect prefix hijacking and other anomalies.
- In IPv4, at least 2.85% of BAPLs were associated with prefix hijacking or other routing anomalies.
- These BAPLs can be attributed to faulty configurations or intentional attacks.

Outline

- Background
- Data sets and methodology
- Will BAPL lead to forwarding loops?
- Measurement results
  - Total number and ratio of BAPLs
  - Duration of BAPLs
  - Loop length of BAPLs
- Explanations of BAPL
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks
- Conclusion

Conclusion

- BAPLs & forwarding AS path loops.
- Characteristics of BAPL
  - The number and ratio
  - Duration
  - Loop length
- Explanations
  - Private AS number leaking
  - Multinational companies
  - Preventing particular AS from accepting routes
  - Faulty configurations or malicious attacks

Thank you !