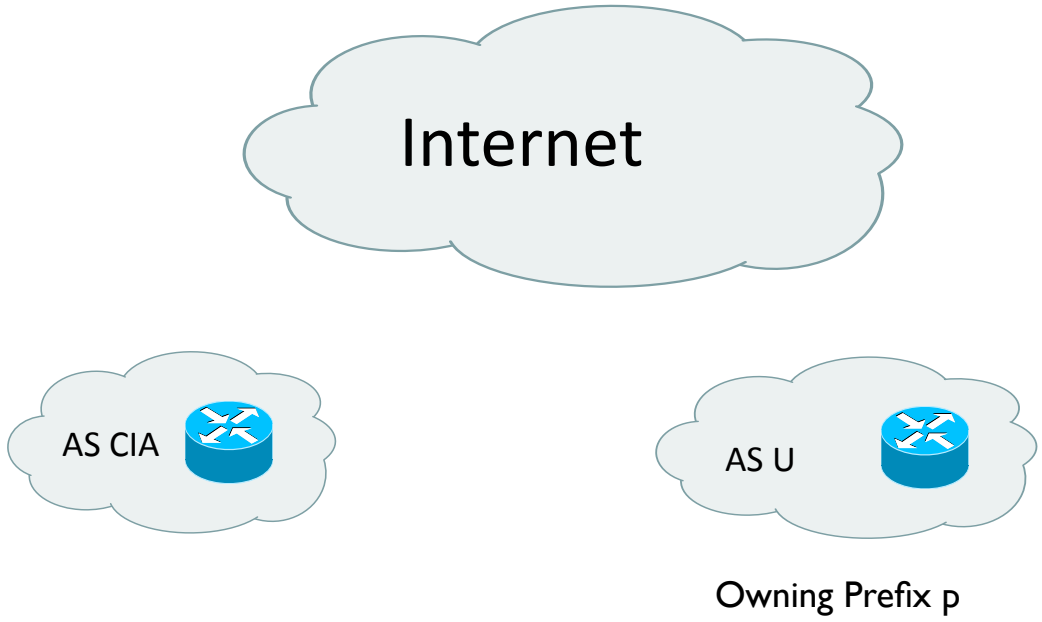
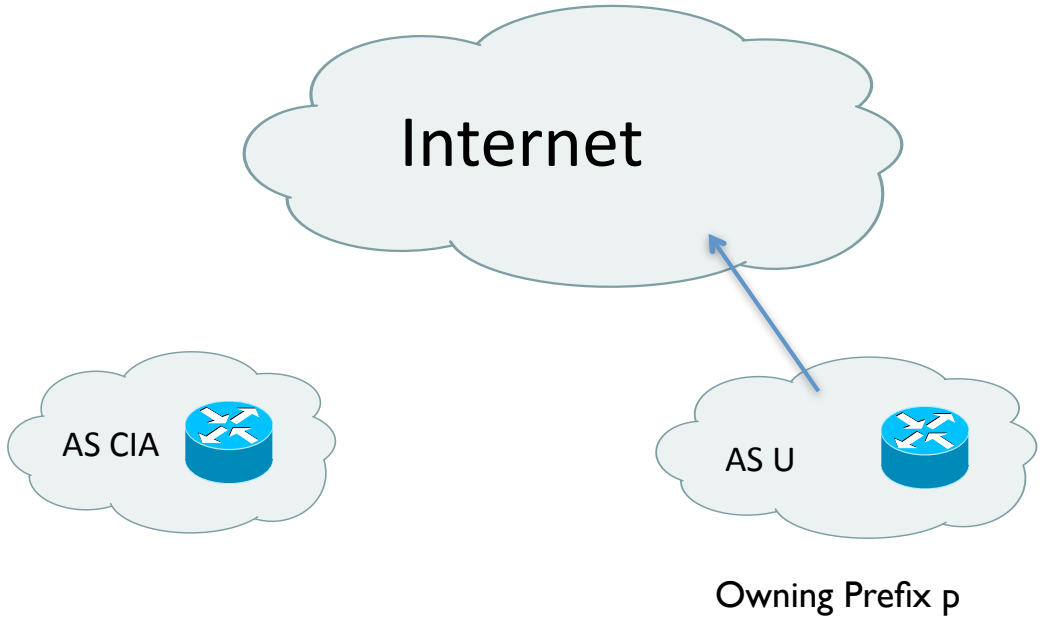
A Study of Prefix Hijacking and Interception in the internet

Hitesh Ballani, Paul Francis, Xinyang Zhang
Presented by: Tony Z.C Huang, Adapted from slides by Hitesh Ballani

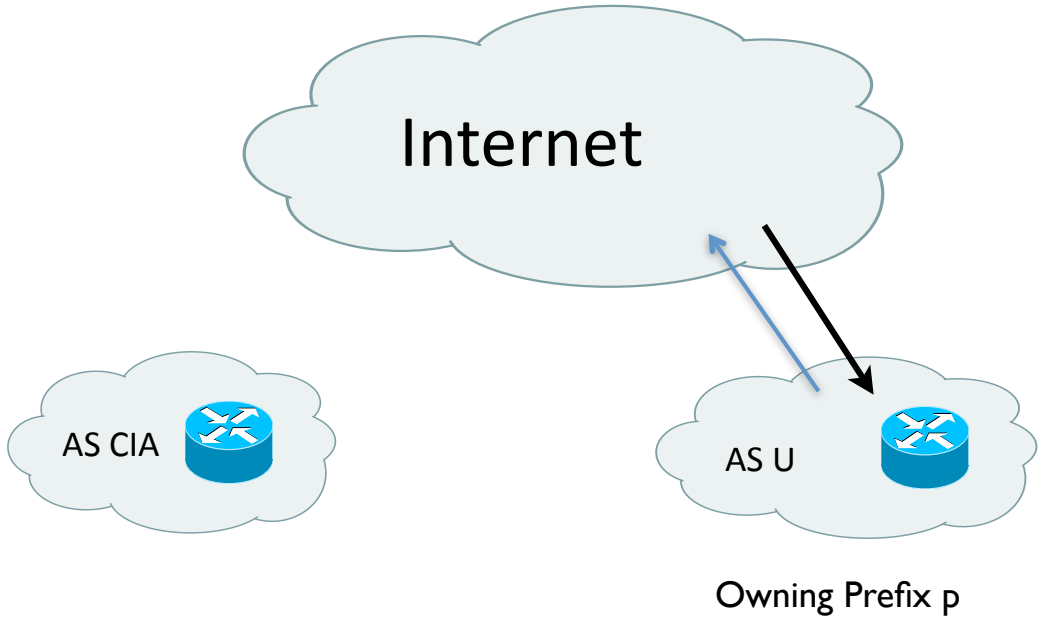
Prefix Hijacking/ Interception



Prefix Hijacking/ Interception

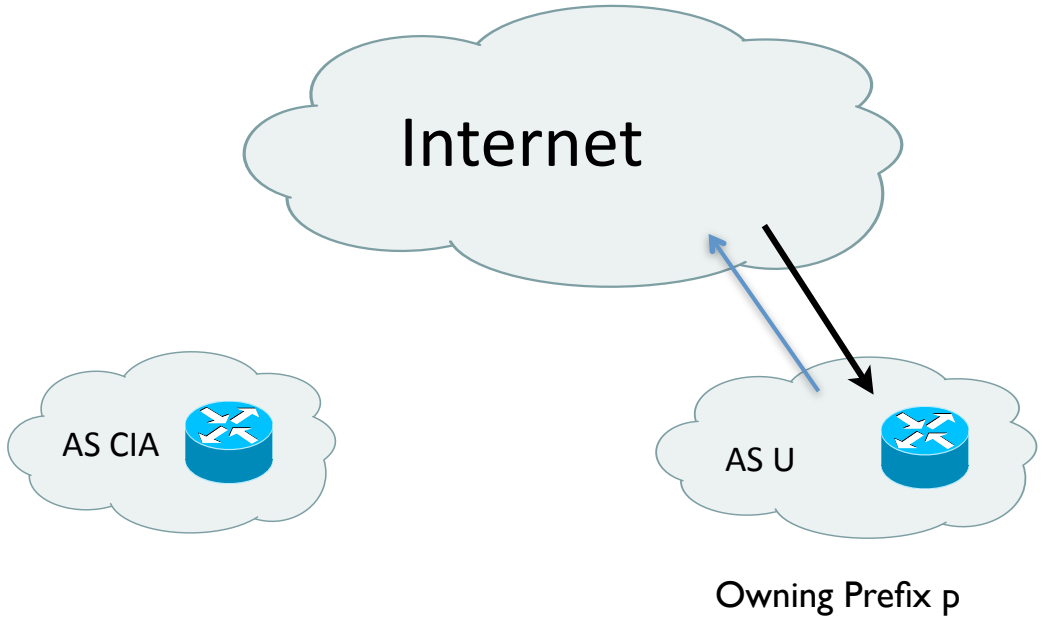


Prefix Hijacking/ Interception



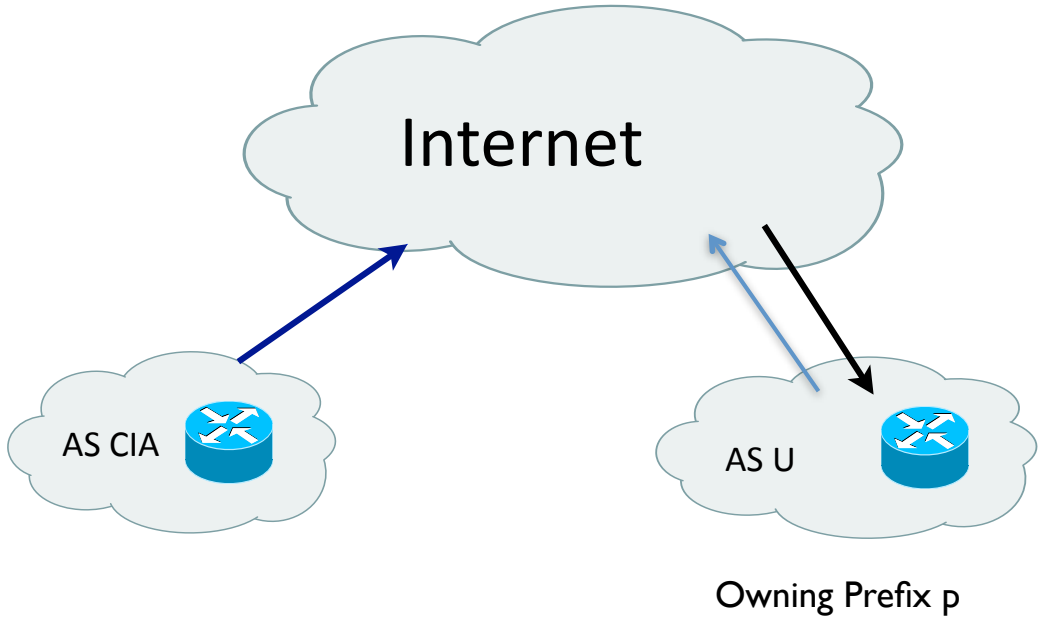
Prefix Hijacking/ Interception

- Prefix Hijacking:AS CIA advertises a prefix owned by AS U.
  - Creates a black-hole in the internet



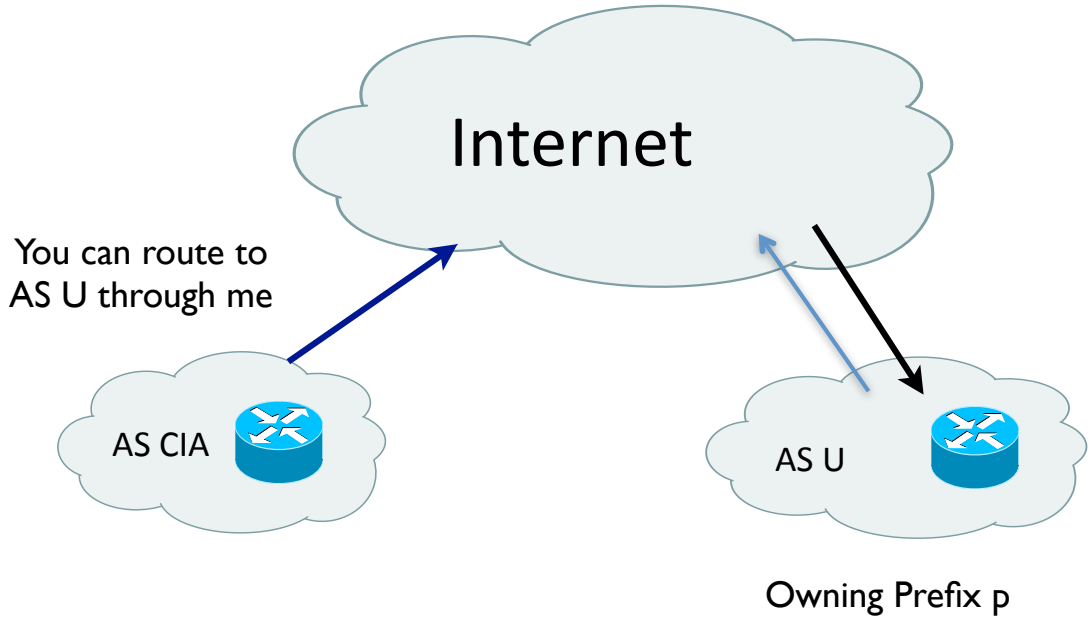
Prefix Hijacking/ Interception

- Prefix Hijacking:AS CIA advertises a prefix owned by AS U.
  - Creates a black-hole in the internet



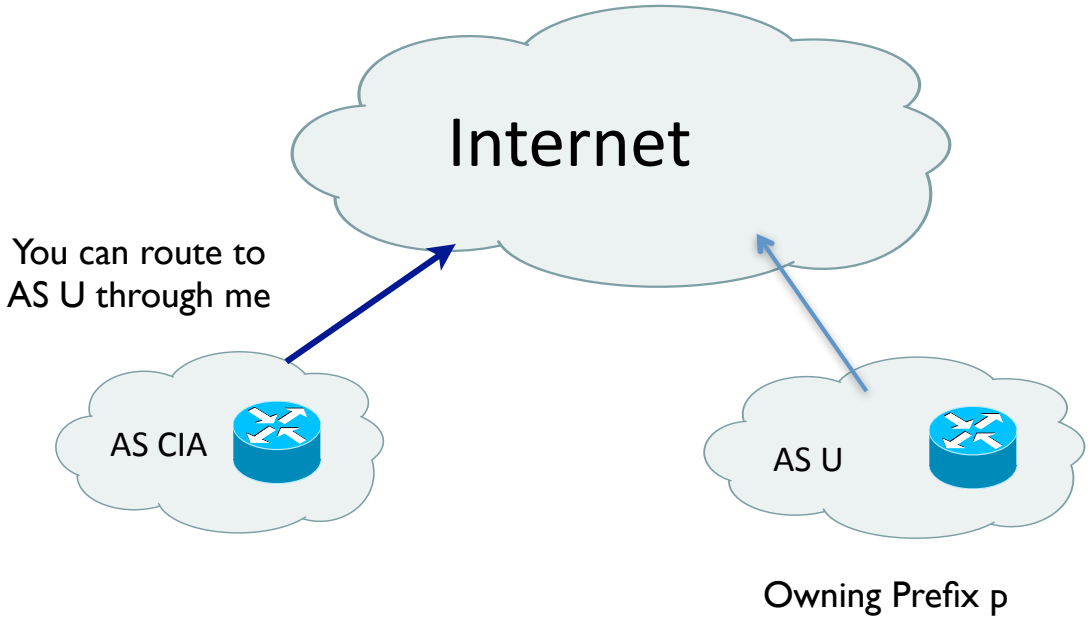
Prefix Hijacking/ Interception

- Prefix Hijacking:AS CIA advertises a prefix owned by AS U.
  - Creates a black-hole in the internet



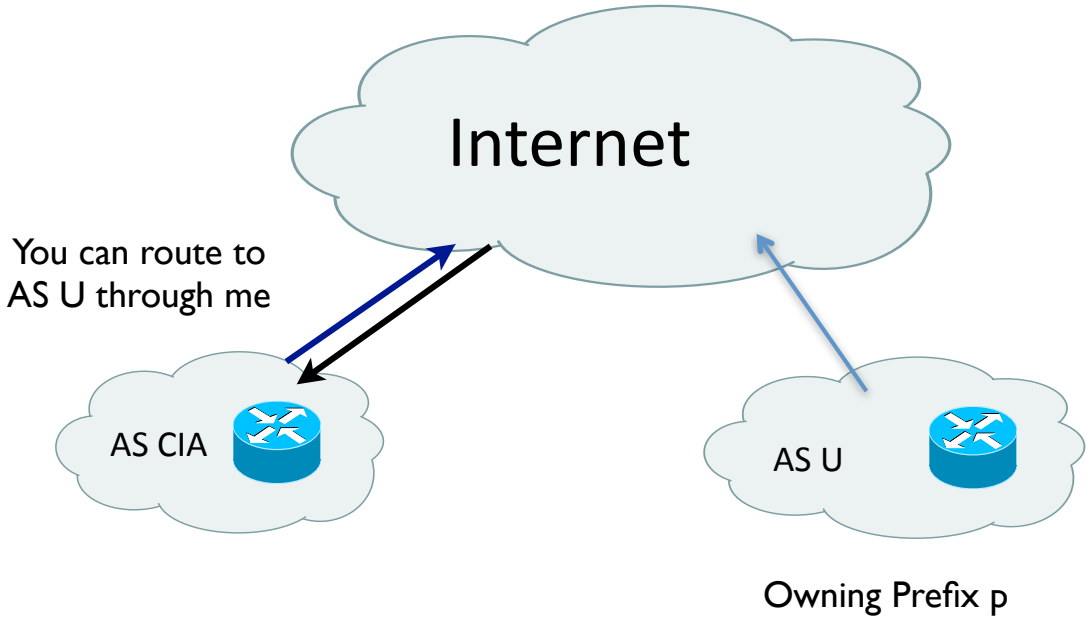
Prefix Hijacking/ Interception

- Prefix Hijacking:AS CIA advertises a prefix owned by AS U.
  - Creates a black-hole in the internet



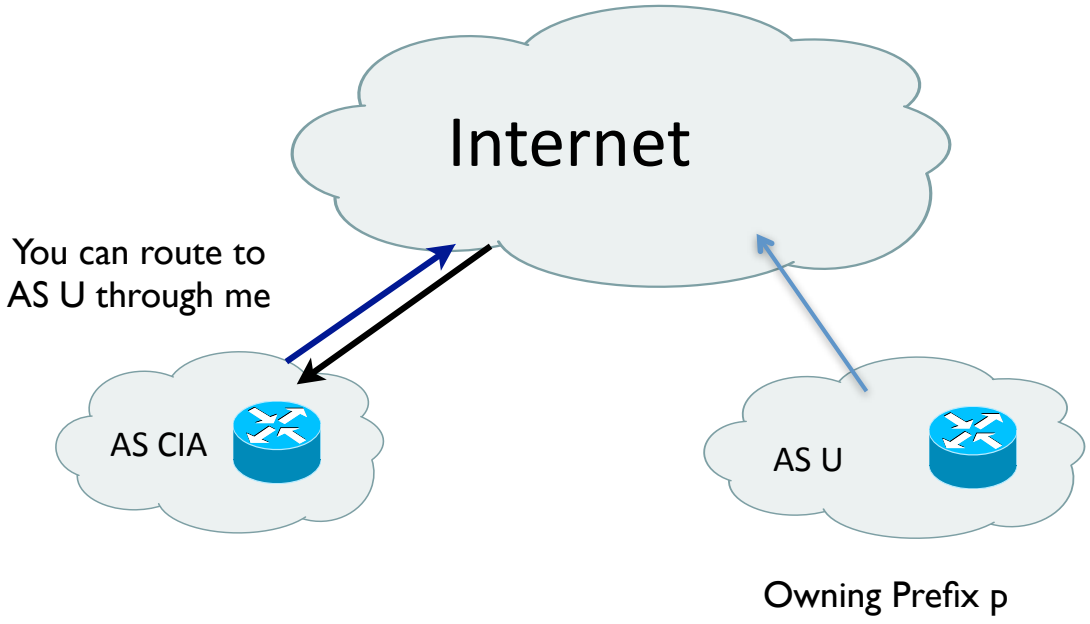
Prefix Hijacking/ Interception

- Prefix Hijacking:AS CIA advertises a prefix owned by AS U.
  - Creates a black-hole in the internet



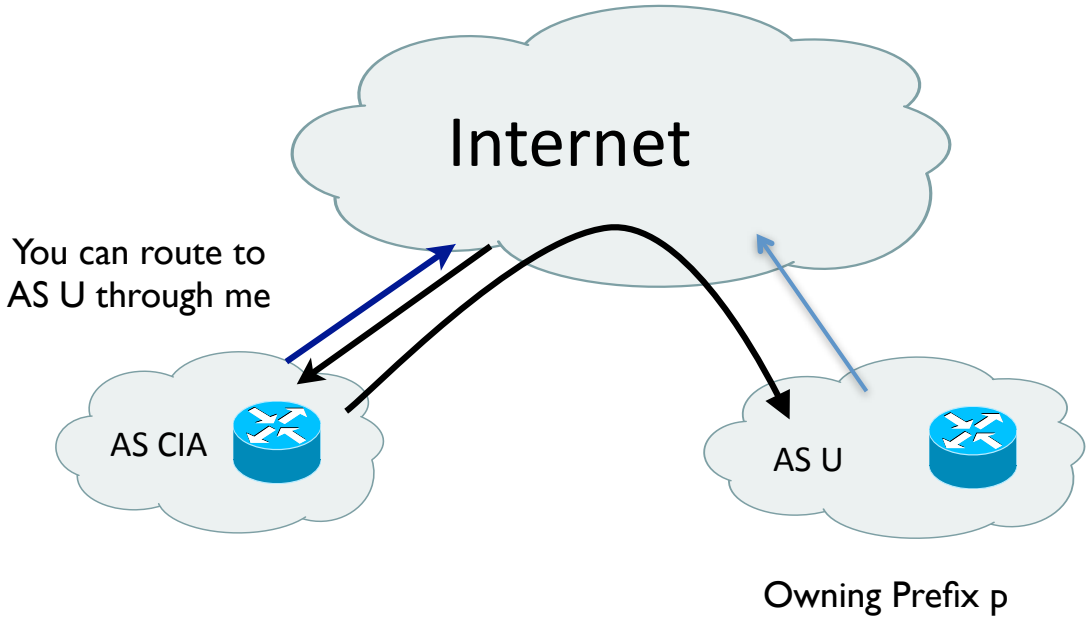
Prefix Hijacking/ Interception

- Prefix Hijacking:AS CIA advertises a prefix owned by AS U.
  - Creates a black-hole in the internet
- Prefix Interception:AS CIA routes the intercepted traffic back to AS U
  - AS U would not find out the traffic has been intercepted.



Prefix Hijacking/ Interception

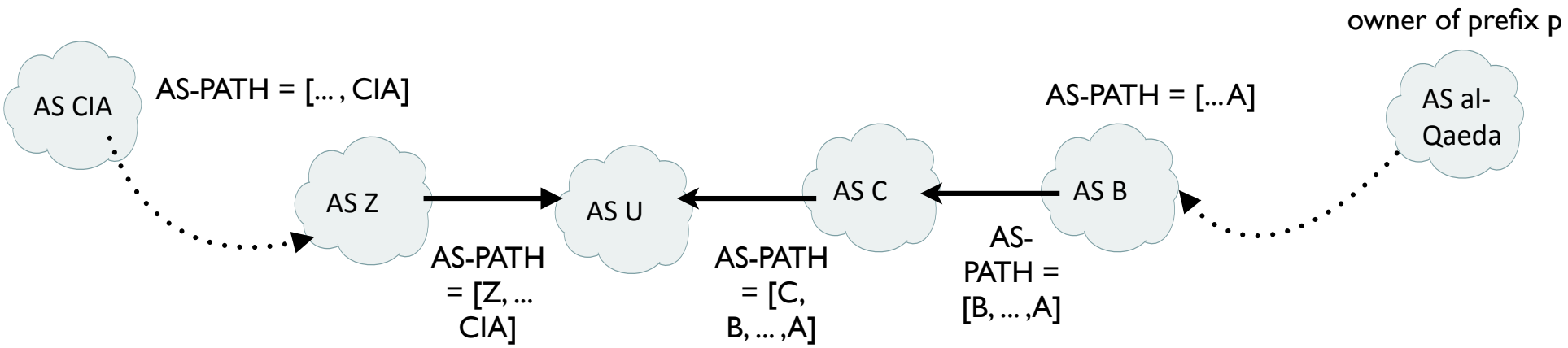
- Prefix Hijacking:AS CIA advertises a prefix owned by AS U.
  - Creates a black-hole in the internet
- Prefix Interception:AS CIA routes the intercepted traffic back to AS U
  - AS U would not find out the traffic has been intercepted.



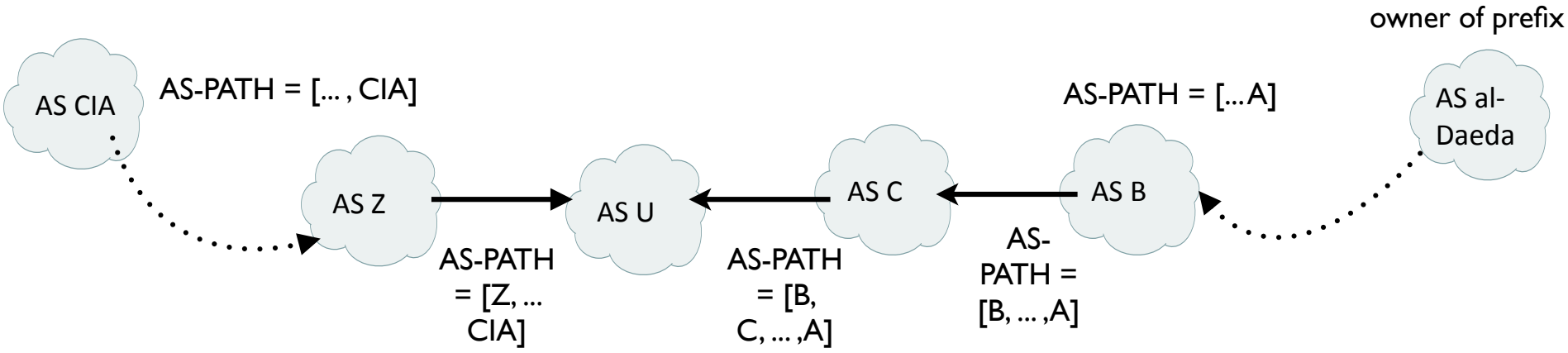
Focus of the paper

- 1) Analyze the probability of traffic hijacking/ Interception.
- 2) Use routing tables from Route-Views, estimate the actual probability that an AS can hijack/ intercept traffics from other ASes.
- 3) Implement interception methodology and intercept real traffic.
- 4) Try to detect actual interception in the internet.

Hijacking Analysis



- Question: Can CIA hijacks prefix p's traffic from AS al-Qaeda?
- AS U Needs to choose between two routes
  - Valid routes: AS-Path = [C,B,... A], length = n;
  - Invalid routes: AS-Path = [Z, ... CIA], length = i;
- Assumption: AS U has typical policies:
  - customer routes > peer routes > provider routes



	Length	Customer	Peer	Provider
Customer	i<n	X	X	X
	i=n	--	X	X
	i>n	Y	X	X
Peer	i<n	Y	X	X
	i=n	Y	--	X
	i>n	Y	Y	X
Provider	i<n	Y	Y	X
	i=n	Y	Y	--
	i>n	Y	Y	Y

- X: The traffic can not be hijacked.
- Y: The traffic can be hijacked.

Discussion

Discussion

- Better way to hijack the traffic?

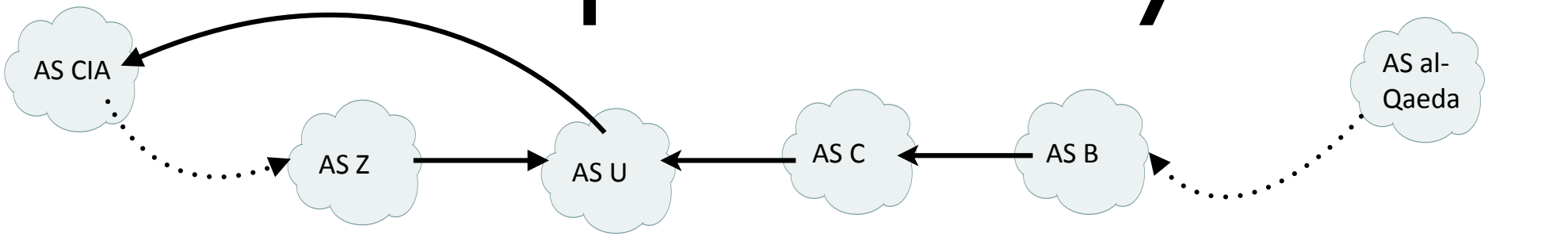
Discussion

- Better way to hijack the traffic?
- Yes, by announcing a more specific prefix.

Discussion

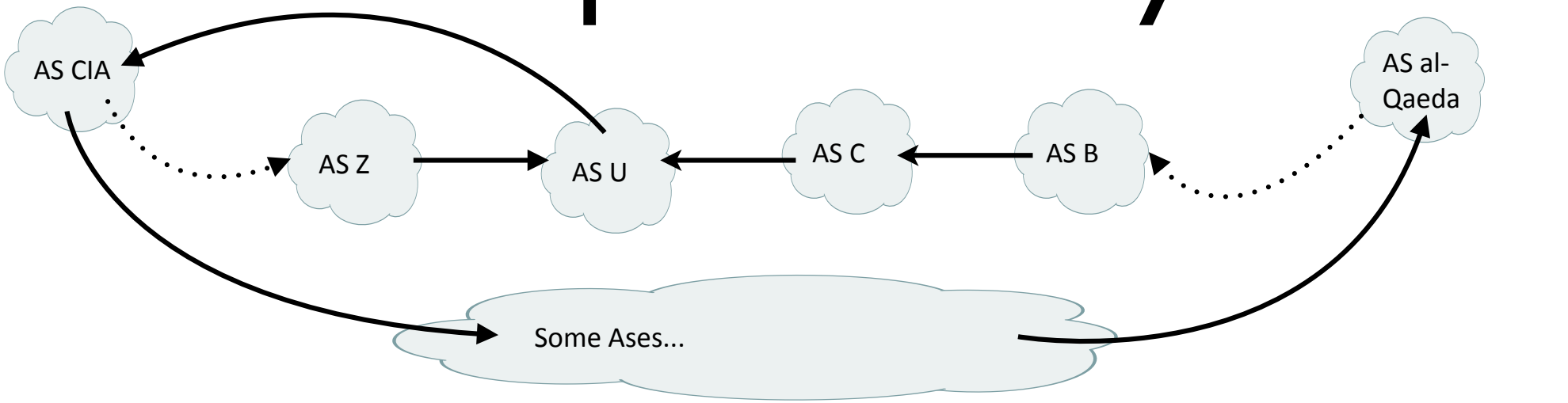
- Better way to hijack the traffic?
- Yes, by announcing a more specific prefix.
- But in practice, BGP filter out prefixes more specific than /24. So analysis in this paper is still useful.

Interception Analysis



- The problem is routing the traffic back to the original As.
- The problem is, if AS CIA's existing routes also switches to the invalid routes, then AS CIA can not route the traffic back to AS al-Qaeda.
- Safety Condition: AS CIA should have a valid route for prefix p during the Interception.

Interception Analysis



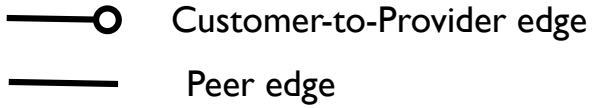
- The problem is routing the traffic back to the original As.
- The problem is, if AS CIA's existing routes also switches to the invalid routes, then AS CIA can not route the traffic back to AS al-Qaeda.
- Safety Condition: AS CIA should have a valid route for prefix p during the Interception.

Interception Analysis

- Two assumptions
  - customer routes > peer routes > provider routes
  - "Valley-free" property
    i.e, after traversing a provider-to-customer edge or a peer edge, the path cannot traverse another customer-to-prover or peer edge.

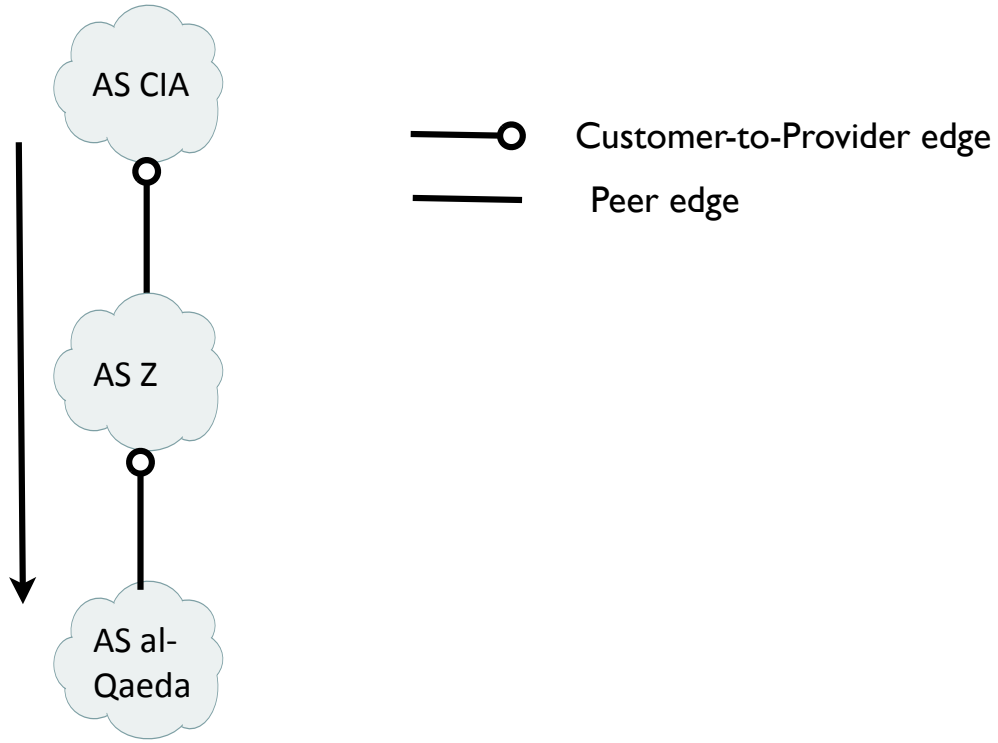
Interception Analysis

- Case 1, AS CIA's current route is a customer routes. Namely, AS al-Qaeda is a customer of AS-CIA.
- Conclusion: AS-CIA can advertise the invalid route to all its neighbors, and still satisfies the safety condition.



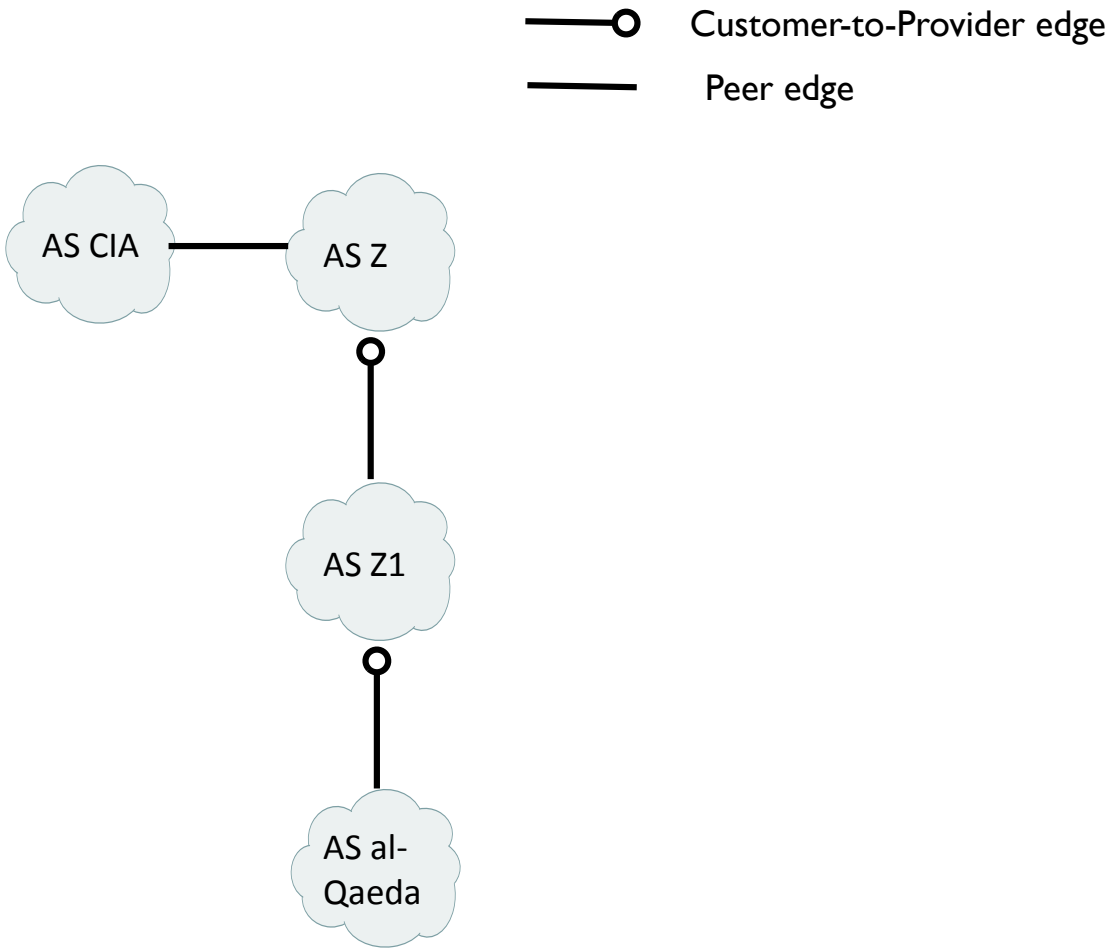
Interception Analysis

- Case 1, AS CIA's current route is a customer routes. Namely, AS al-Qaeda is a customer of AS-CIA.
- Conclusion: AS-CIA can advertise the invalid route to all its neighbors, and still satisfies the safety condition.



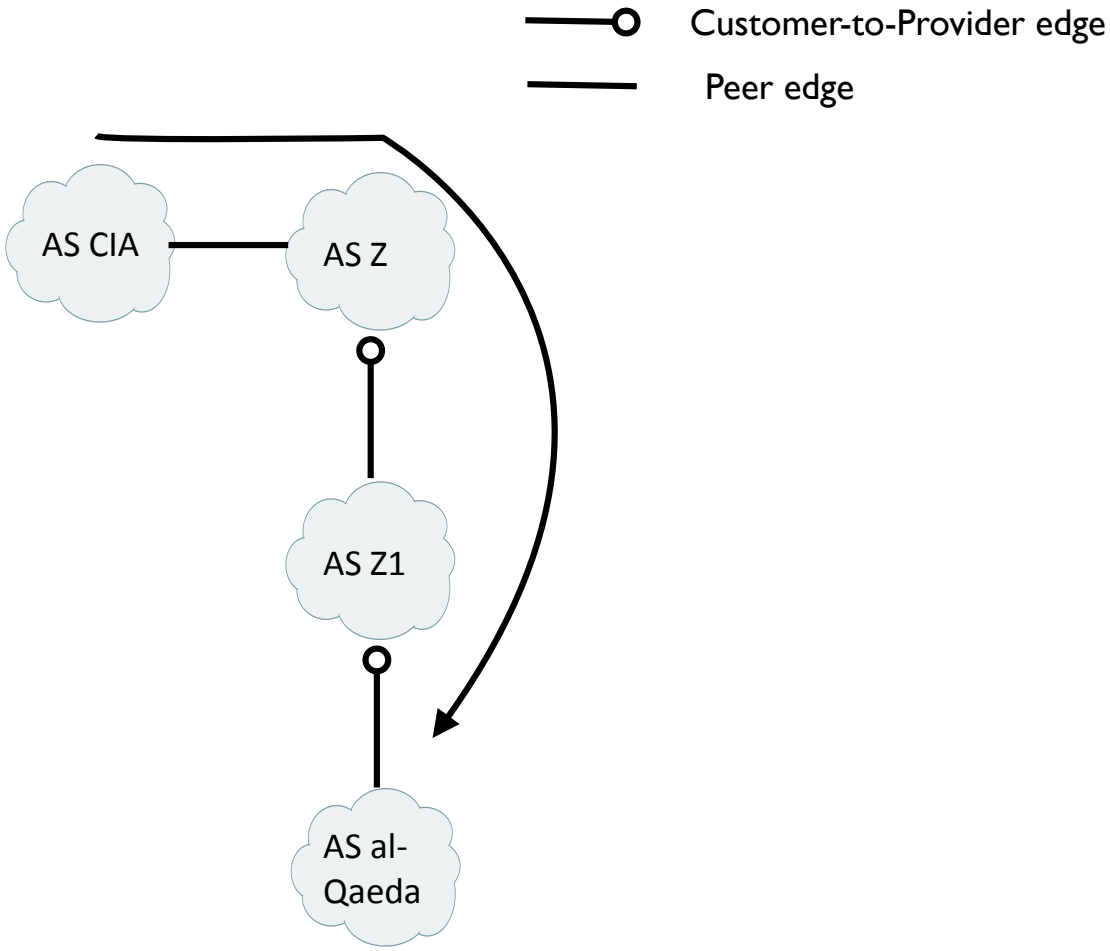
Interception Analysis

- Case II, AS CIA's current route is a peer routes. Namely, AS al-Qaeda is a peer of AS-CIA.
- Conclusion: Similar to Case I, AS CIA can propagate to any of the ASes along the path without violating the safety condition.



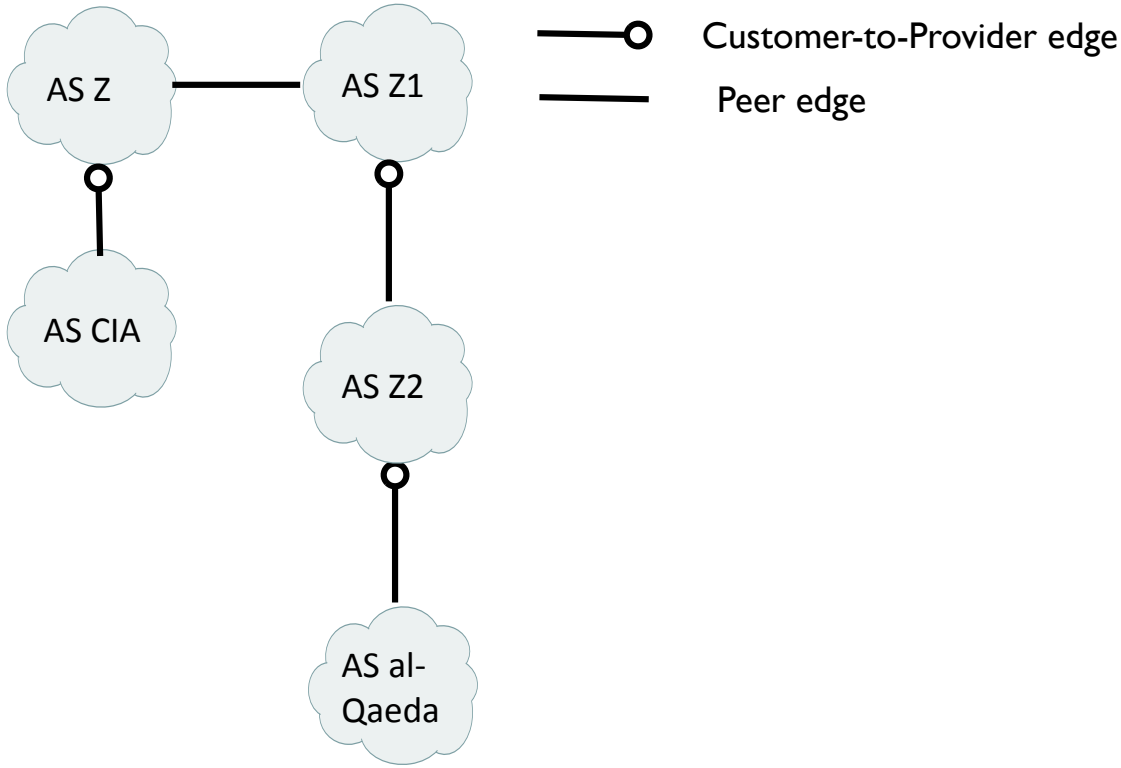
Interception Analysis

- Case II, AS CIA's current route is a peer routes. Namely, AS al-Qaeda is a peer of AS-CIA.
- Conclusion: Similar to Case I, AS CIA can propagate to any of the ASes along the path without violating the safety condition.



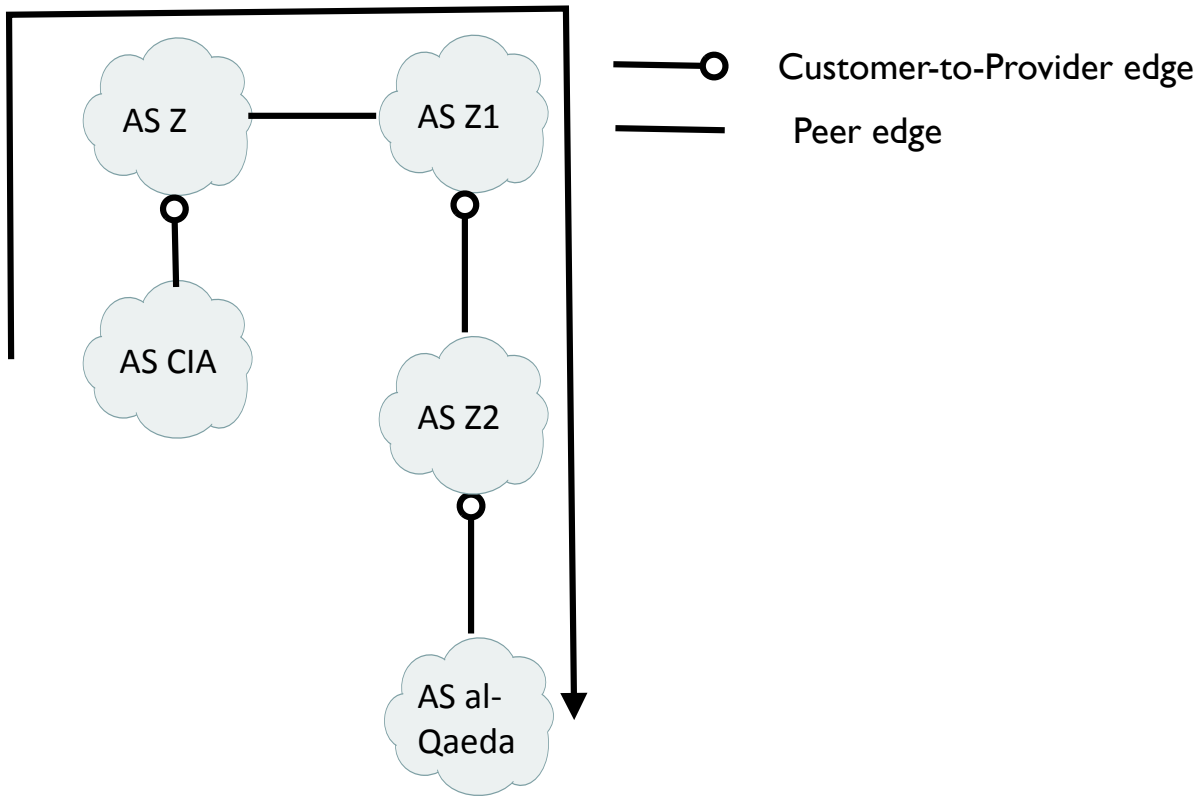
Interception Analysis

- Case III, AS CIA's current route is a provider routes.
- Conclusion: AS CIA can only advertises the path to its customer and peers, but not to its provider.



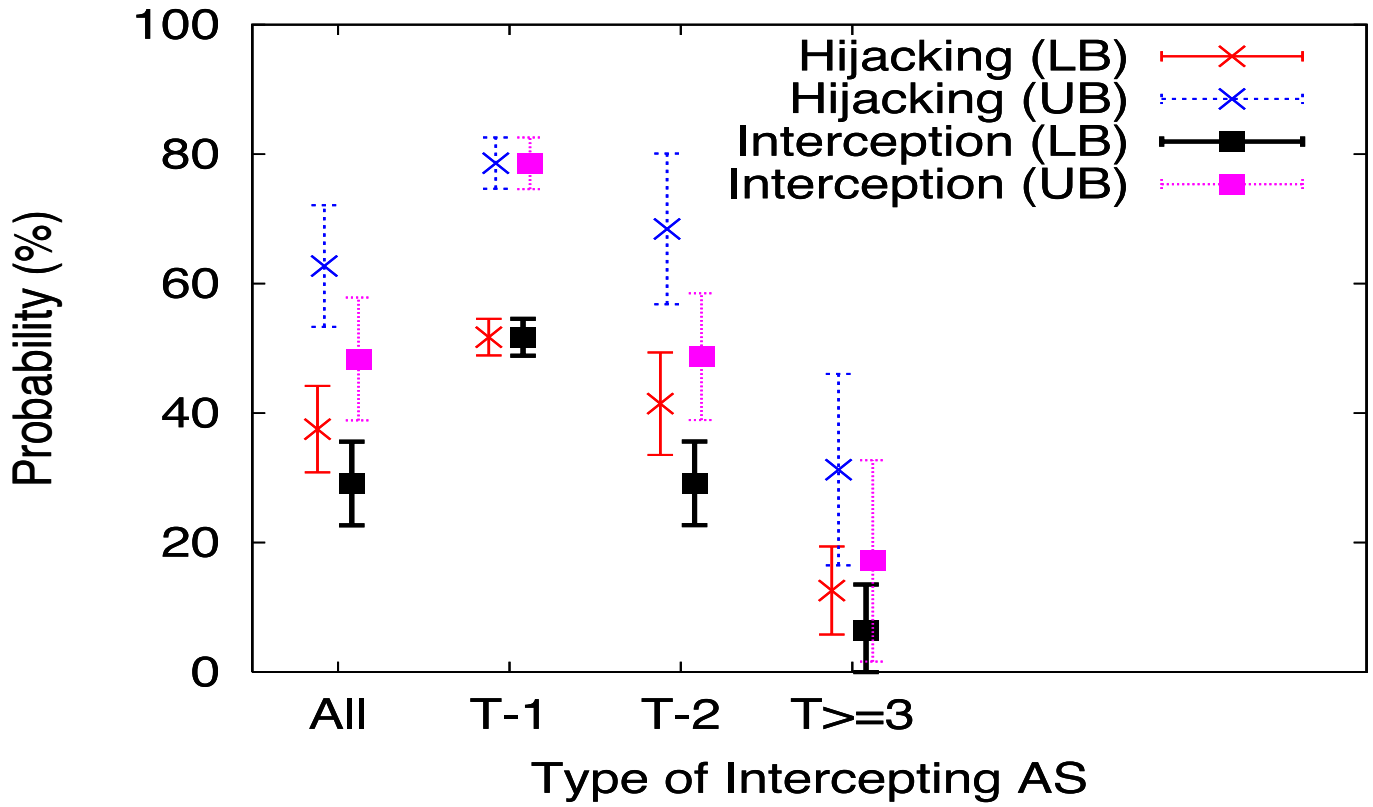
Interception Analysis

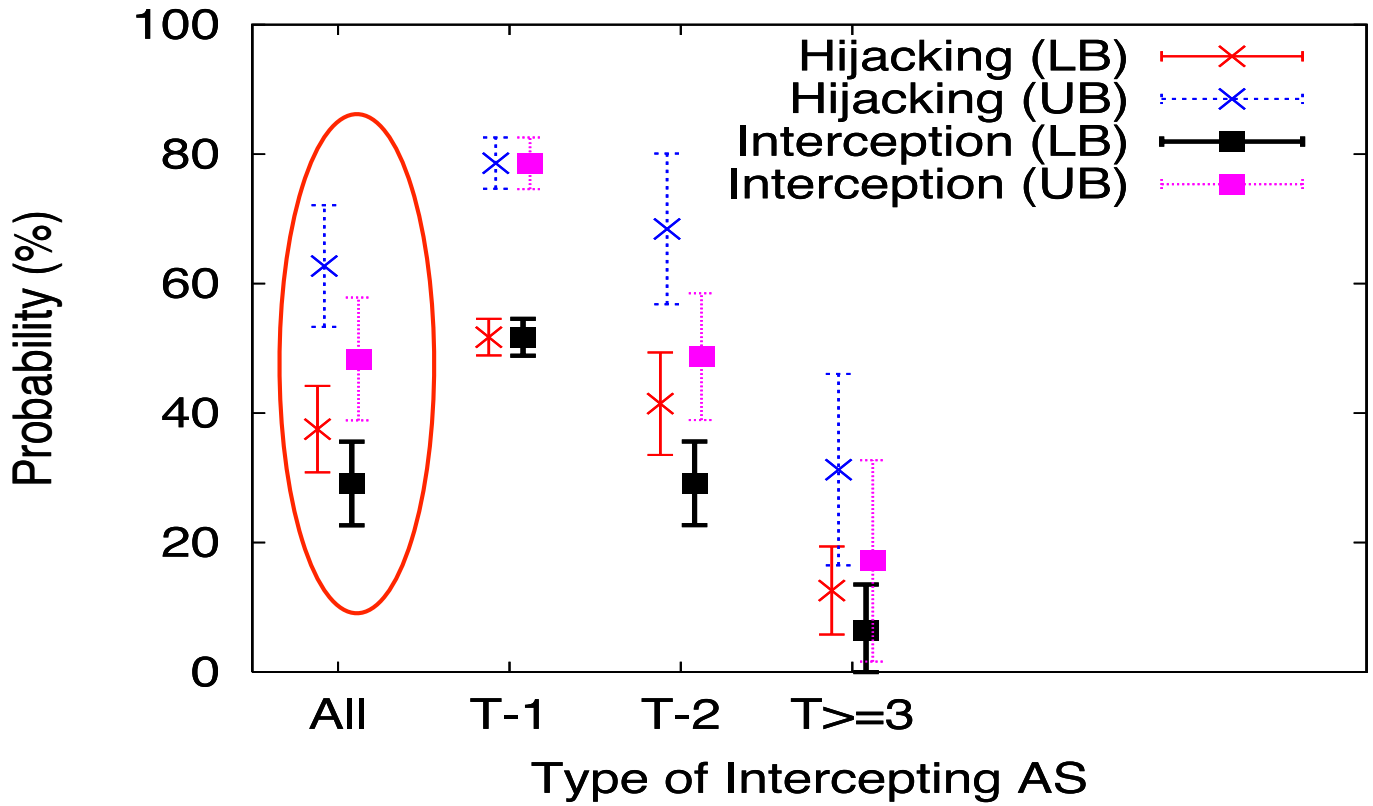
- Case III, AS CIA's current route is a provider routes.
- Conclusion: AS CIA can only advertises the path to its customer and peers, but not to its provider.



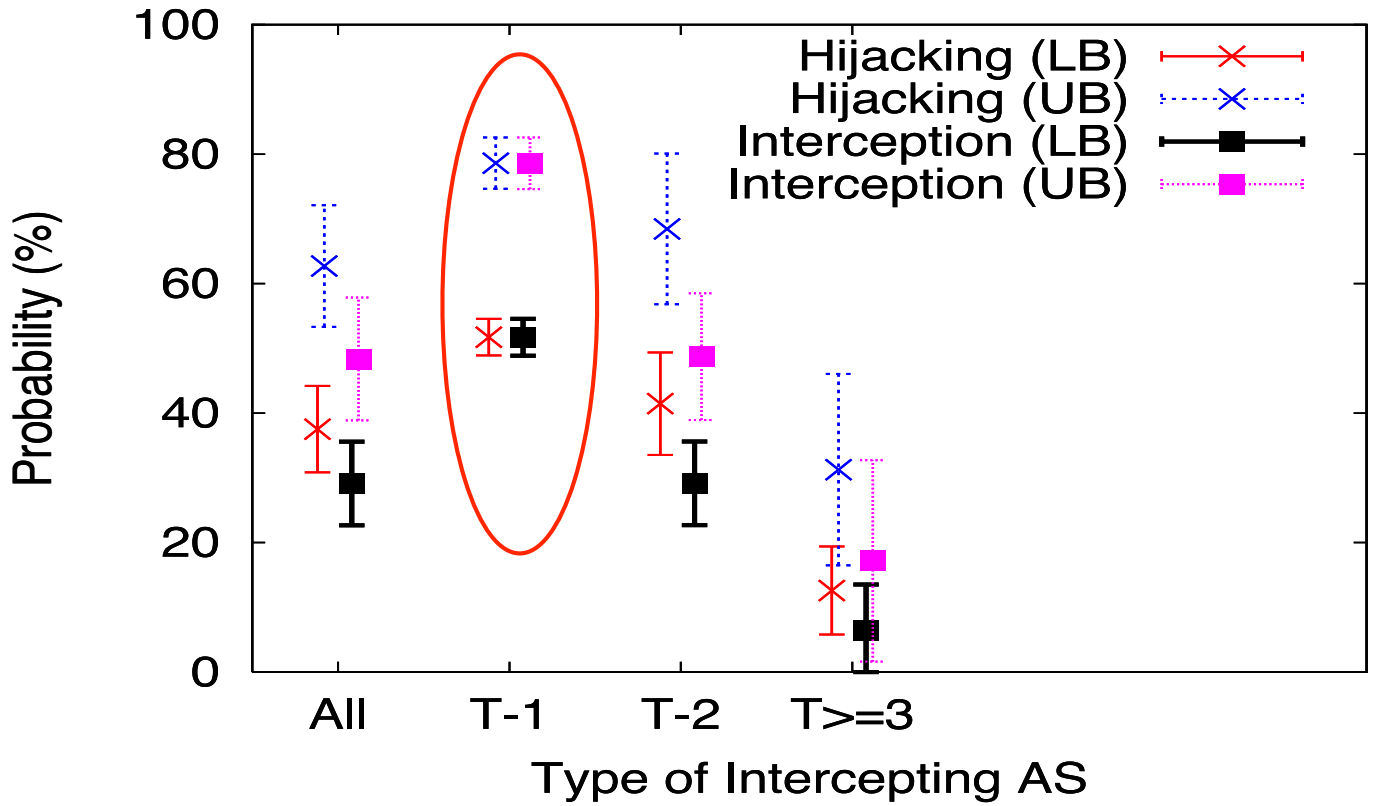
Hijacking/Interception Estimate

- Analysis results applied to Route-Views ASes
  - Route-view repository comprised of 34 ASes (RV-Set)
  - 7 tier-1 ASes, 19 tier-2, 8 others.
- Parameter of Interest
  - Probability of Hijacking: Fraction of ASes whose traffic is hijacked by the hijacking AS, averaged across all ASes and all prefixes.
  - Probability of Interception is defined similarly.

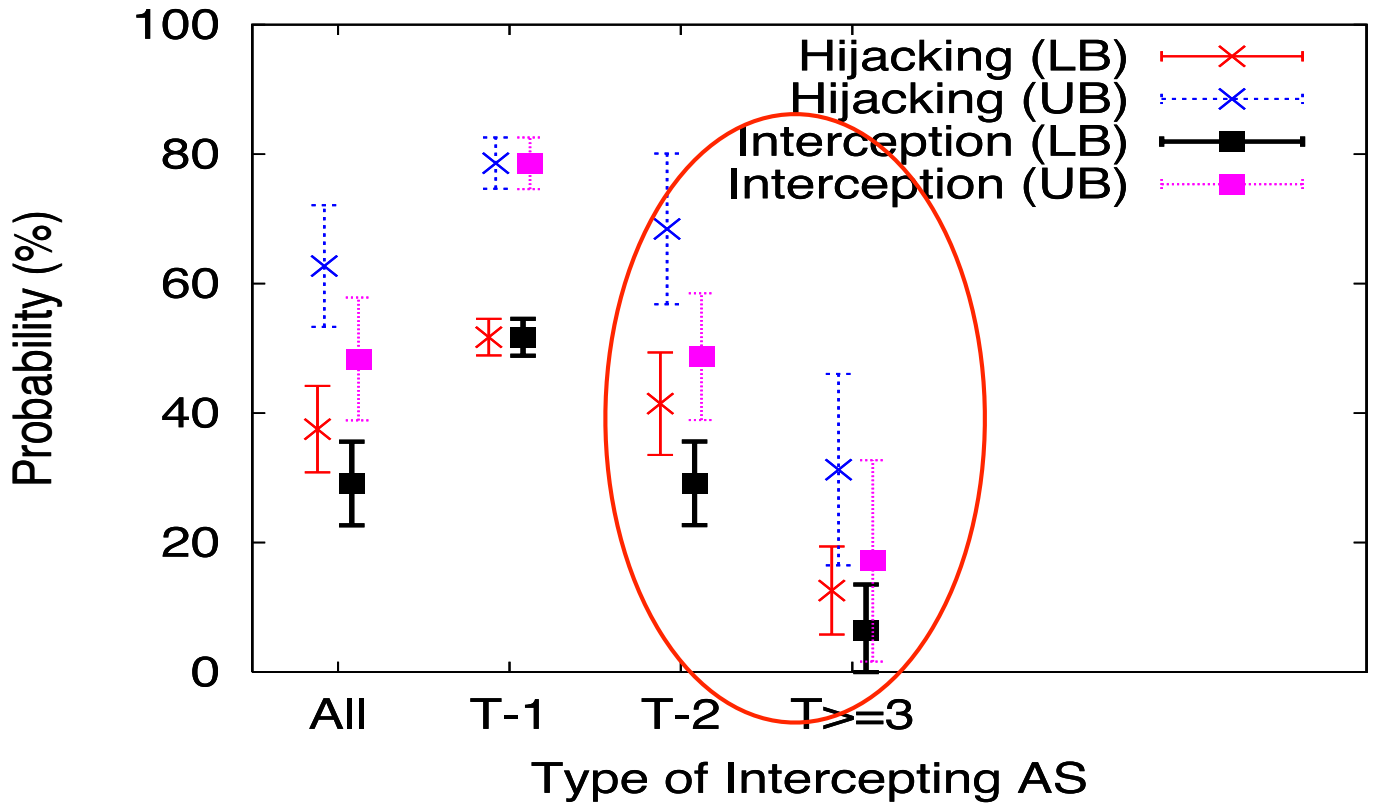

100
80
60
40
20
0
Probability (%)
All
T-1
T-2
T>=3
Type of Intercepting AS
Hijacking (LB)
Hijacking (UB)
Interception (LB)
Interception (UB)



- Probability of hijacking ~ 40-60%
- Probability of interception ~ 30-50%

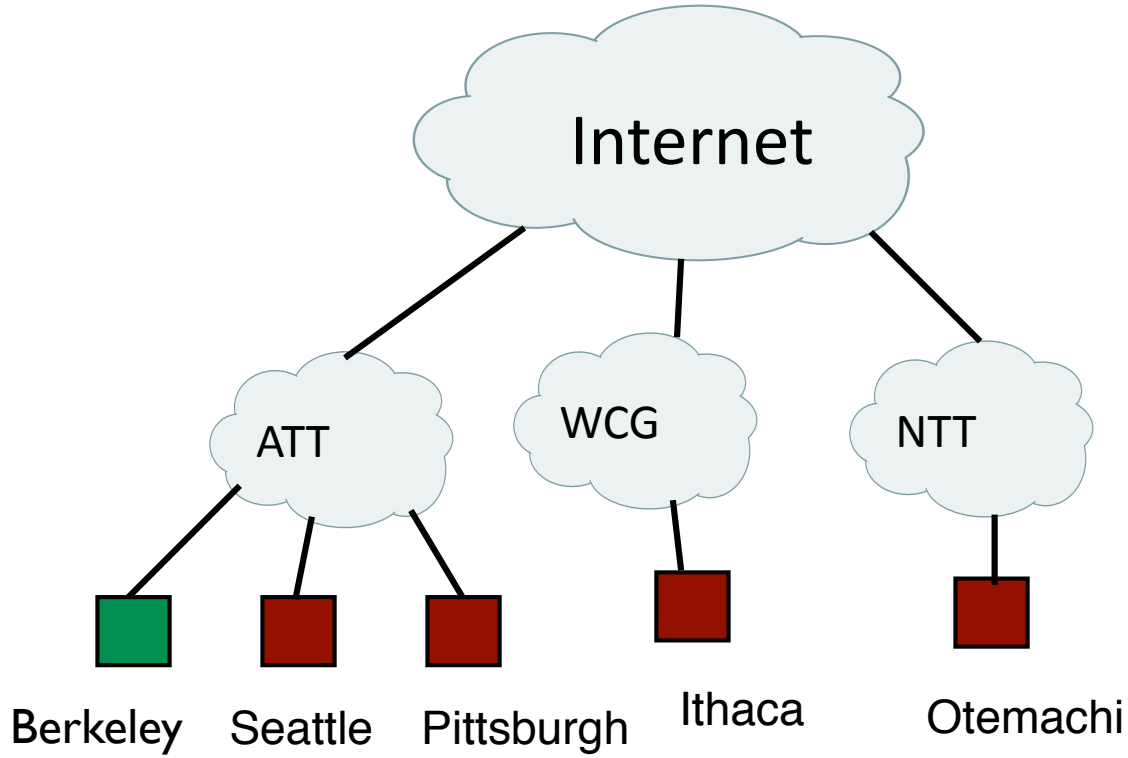


- Probability of hijacking for tier-1 ISPs ~ 50-80%
- Probability of interception for tier-1 ISPs ~ 50-80%


100
80
60
40
20
0
Probability (%)
All
T-1
T-2
T>=3
Type of Intercepting AS
Hijacking (LB)
Hijacking (UB)
Interception (LB)
Interception (UB)

Hijacking/Interception Real Traffic

- Hijacking Experiment: Have one of the server acts as owner of the prefix, and other 4 servers try to hijack the traffic.
- Interception Experiment: Have two of the servers intercepts the traffic and routes the traffic back to the owner using the other two server.



Ber	Pit	Sea	Ith	Ote	% of traffic Hijacked	% of traffic Intercepted
O	✗	✗	✓	✓	91.7	78.8
✗	O	✗	✓	✓	68.8	67.5
✗	✗	O	✓	✓	97.4	66.2
✗	✗	✗	O	✓	66.0	47.3
✓	✓	✓	✗	O	76.1	23.4

O : Site owning the prefix
✗ : Site not advertising an invalid route during interception
✓ : Site advertising an invalid route during interception

Discussion

Discussion

- Is prefix-hijack preventable under the current internet architecture?

Discussion

- Is prefix-hijack preventable under the current internet architecture?
- Generally, is prefix-hijack preventable under a fully distributed architecture? How about centralized/semi-centralized architecture?

Discussion

- Is prefix-hijack preventable under the current internet architecture?
- Generally, is prefix-hijack preventable under a fully distributed architecture? How about centralized/semi-centralized architecture?
- Among all the new architecture we have seen (NIRA, Pathlet, MINT, DONA), which one will help defend against prefix-hijacking? which one will make it worse? Makes no differences?