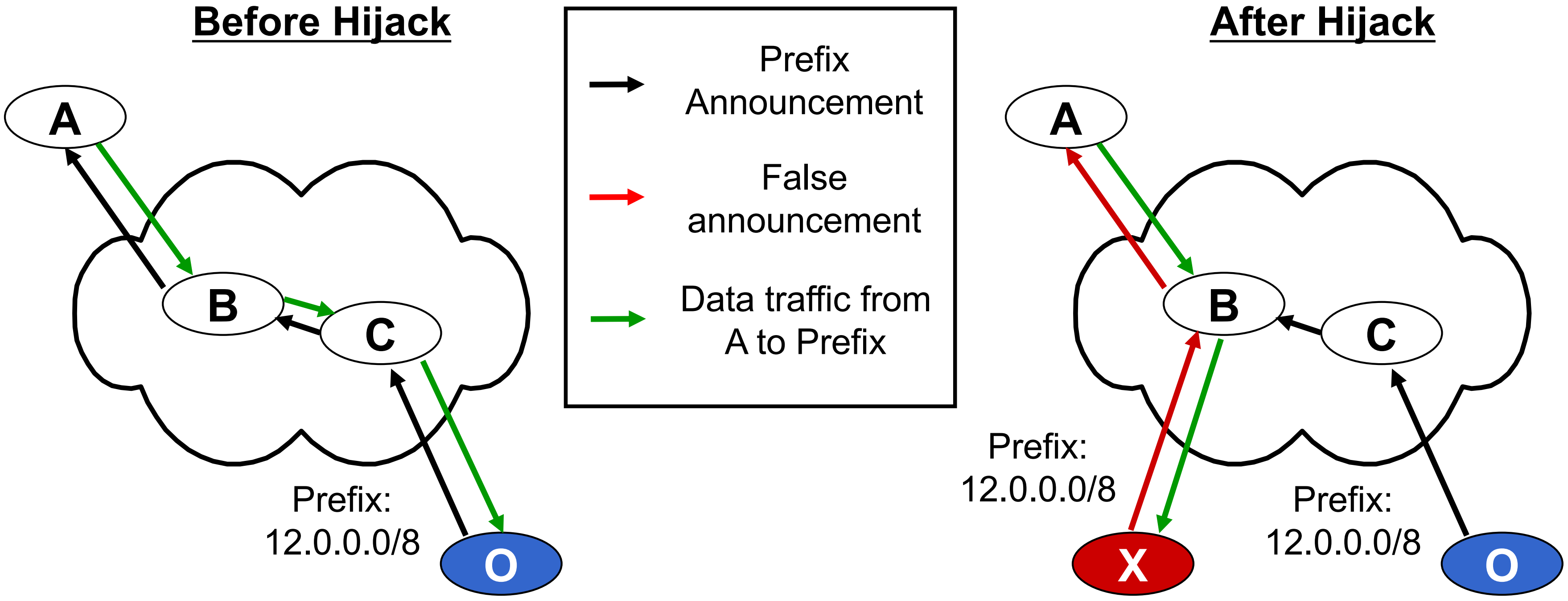
CSC 525:
Principles of Computer Networks

Routing Security

- Not very good.
  - Security was not even on the list of design goals of the original Internet.
- No good way to verify the content of routing announcements.
  - One can fake the prefix origin.
  - One can also fake the path leading to the origin.
  - And the receiving router will just believe it.
- Operational Practice:
  - Protect the access of the router
  - Protect the BGP session between neighbor routers
  - Keep router configuration updated
  - Watch it closely

Prefix Hijack

- Making false routing announcements to attract other's traffic.



Before Hijack

A

B

C

O

Prefix: 12.0.0.0/8

Prefix Announcement

False announcement

Data traffic from A to Prefix

After Hijack

A

B

C

X

Prefix: 12.0.0.0/8

O

Prefix: 12.0.0.0/8

It actually happens …

- Many incidents in the past
  - Sometimes they're called "route leak".
  - 1997: MAI (AS 7007) hijacked the entire Internet
  - 2004: Turkish Telecom (AS 9121) hijacked 70% of the net
  - 2008: Pakistan Telecom (AS 17557) hijacked a YouTube prefix, causing service outage.
  - Many other incidents, happening every year.
- Causes:
  - Misconfigurations
  - Malicious attacks

An incident: Denial of Service

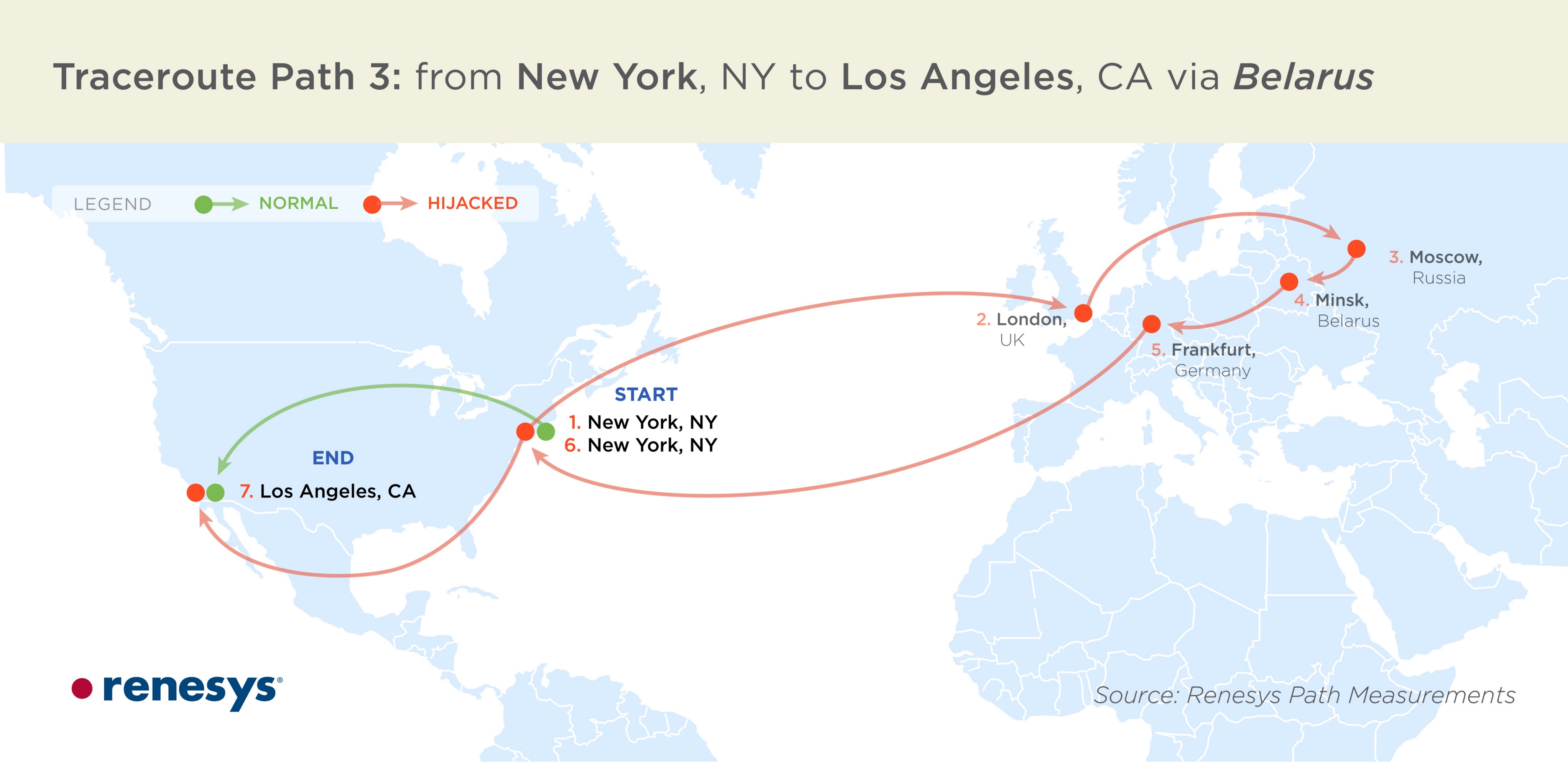
- On Feb 24, 2008, YouTube suffered a global outage for more than two hours.
- Its traffic was hijacked by Pakistan Telecom
  - All YouTube requests were sent towards Pakistan Telecom and then dropped to floor.
  - Intentional hijack to block YouTube within Pakistan.
  - But leaked to the world through its Hong Kong ISP.
- At the time YouTube was using a /22 prefix which was hijacked. YouTube's temporary fix was to split it to 4 /24 prefixes and announced them. This got the traffic to YouTube because of longest prefix match in routing lookup. Eventually they were able to contact the Hong Kong ISP to stop the false routing announcement.

Another incident: imposture

- In Feb 2014, bitcoin mining sites were hijacked multiple times
  - i.e., hosting service by Amazon, Alibaba, Digital Ocean.
  - Each hijack lasted 30s, but repeated 22 times over weeks.
- Hijacked traffic was directed to a Canadian ISP in Montreal.
  - Attacks performed to change bitcoin mining configuration.

Yet another one: man-in-the-middle

- From March to May, 2013, traffic of many sites was redirected to Belarus or Iceland before sending back to the original destination.



Source: Renesys Path Measurements

What Can Be Falsified

- Example:
  - Legit AS path from UA to YouTube prefix 208.65.152.0/22
    - [1706 4323 36561]
- An attacker X can announce
  - The same prefix 208.65.152.0/22
  - A sub-prefix 208.65.152.0/24
  - A super-prefix 208.65.152.0/20
  - An unused prefix
  - An unallocated prefix
- The false path can have
  - False Origin: 1706, X
  - False last-hop: 1706, X, 36561
  - Other false hops: 1706, X, 4323, 36561

What damages it can cause

- Blackhole – Attacker drops all hijacked packets
  - See the known past incidents
- Imposture – Attacker responds to hijacked traffic
  - E.g., research has observed correlation between spam activity and the announcement of short-lived unused prefixes.
- Interception – Attacker forwards the traffic to the target prefix after viewing or modifying the information
  - Could be used as man-in-the-middle attack.
  - Very difficult to detect.

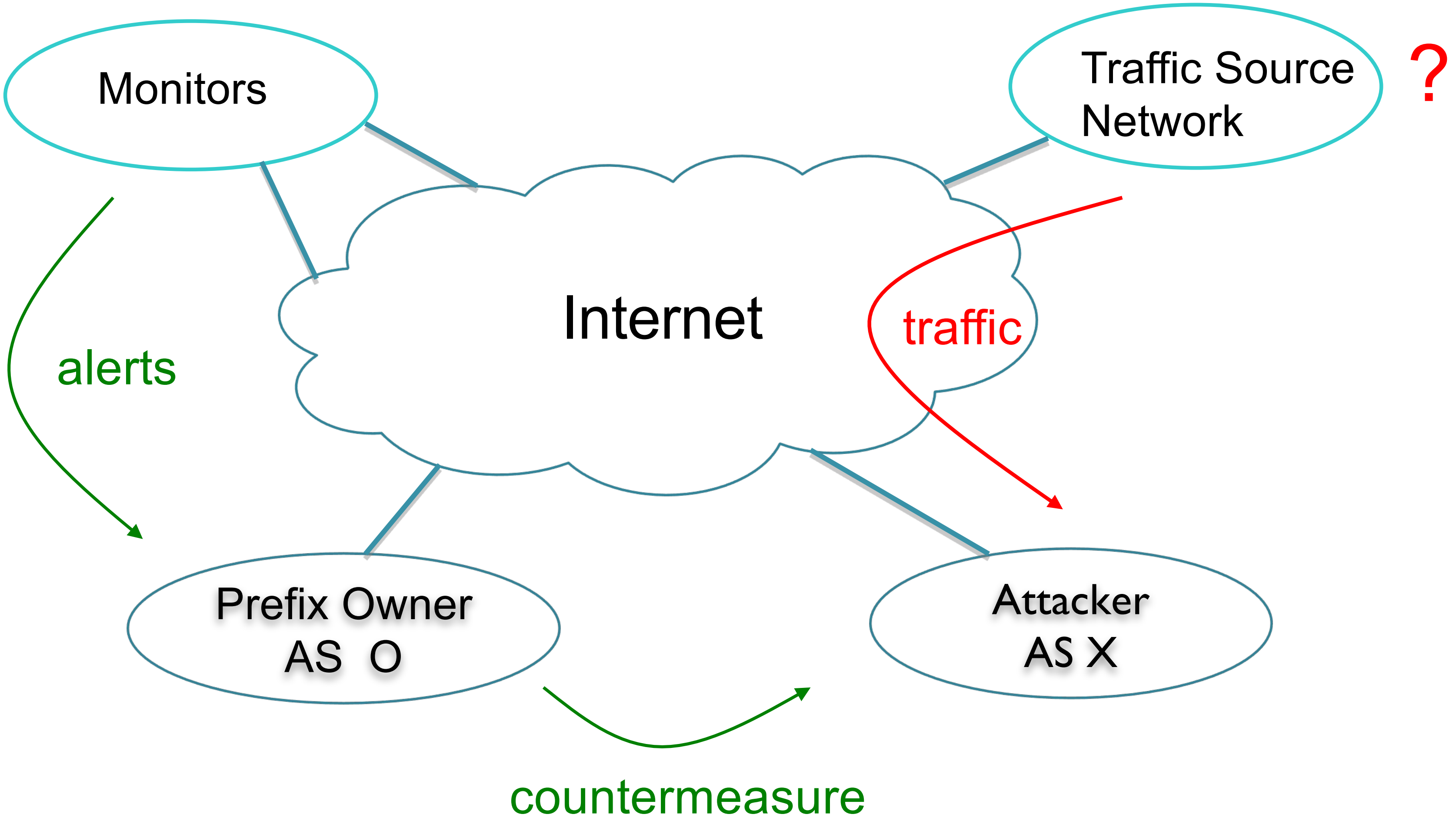
Crypto-based Prevention

- Several proposals to use crypto-based mechanisms to authenticate routing announcements.
  - S-BGP, SoBGP, SIDR, etc.
- Significant computational overhead
- Difficulty in distributing and trusting public keys, i.e., the lack of global PKI (public key infrastructure).

Monitor, Detect, React

- Keep track of what is being announced in global BGP system
  - Real-time data feed through BGP sessions with many ISPs
  - Also analyzing archived historic data
- Ensure your own prefix is accurately represented on the rest of the Internet
- Validating information that you receive by comparing notes with others
  - "given enough eyeballs, all faults will surface"
- Challenge: accuracy and timeliness of the detection.

Different parties in a leak/hijack incident



Current Practice

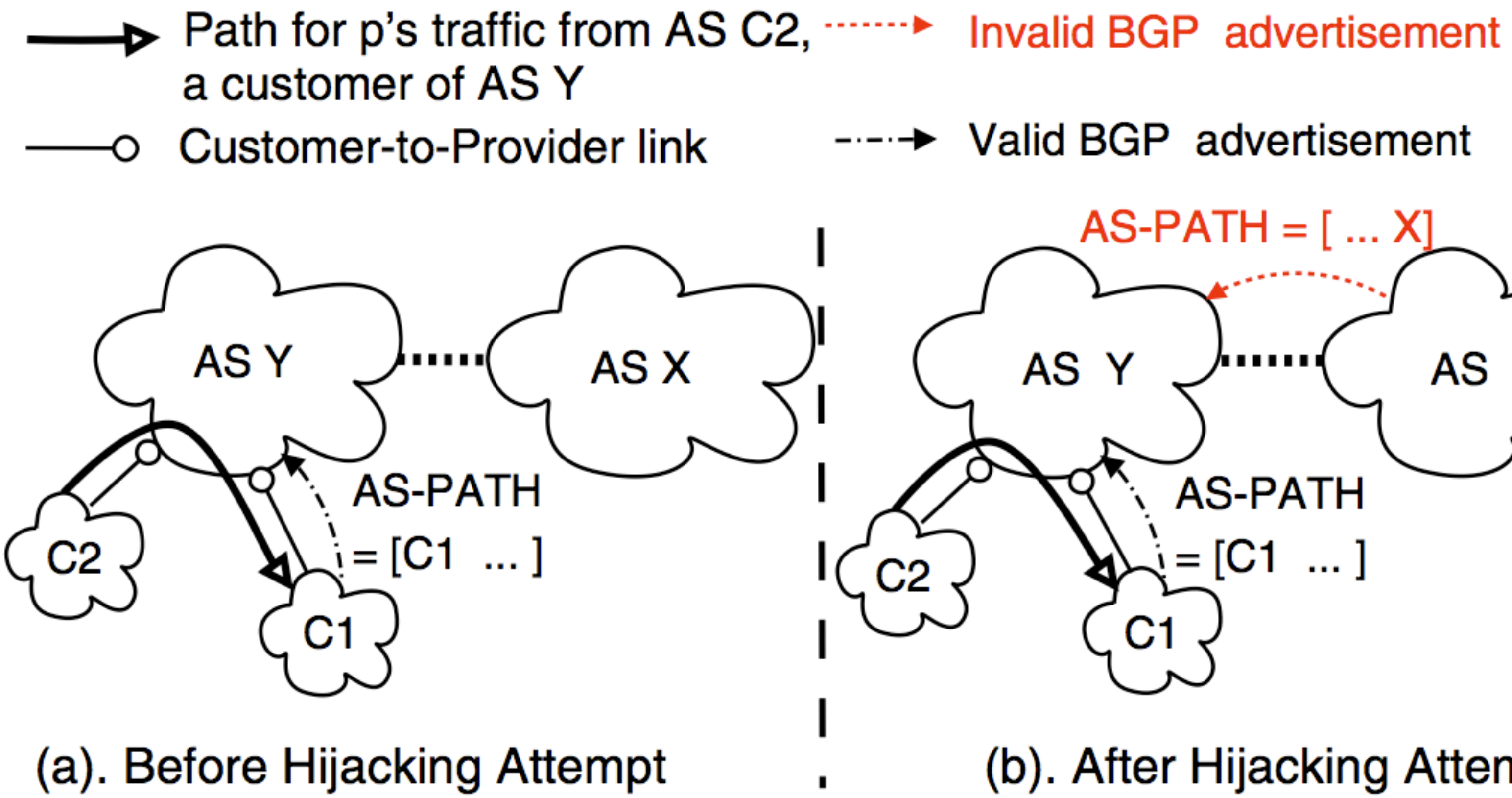
- Hardening the router and its connections.
- Filtering some announcements from neighbors
  - Filter out unallocated prefixes
  - Filter out unregistered prefixes originated from stub customers.
- Limiting the max number of prefixes that a neighbor can send within a short while.
- De-aggregating own prefixes to deal with sub-prefix hijacks.
- Most importantly, having a BGP expert standby.

This Paper

- Analyzing and quantifying the scope of blackhole and interception attacks.
- Conducting an experiment of interception attack on the real Internet.
- Attempting to detect ongoing interception attacks.

- A good example of analyzing Internet routing with routing policy in mind.

Unsuccessful Hijack

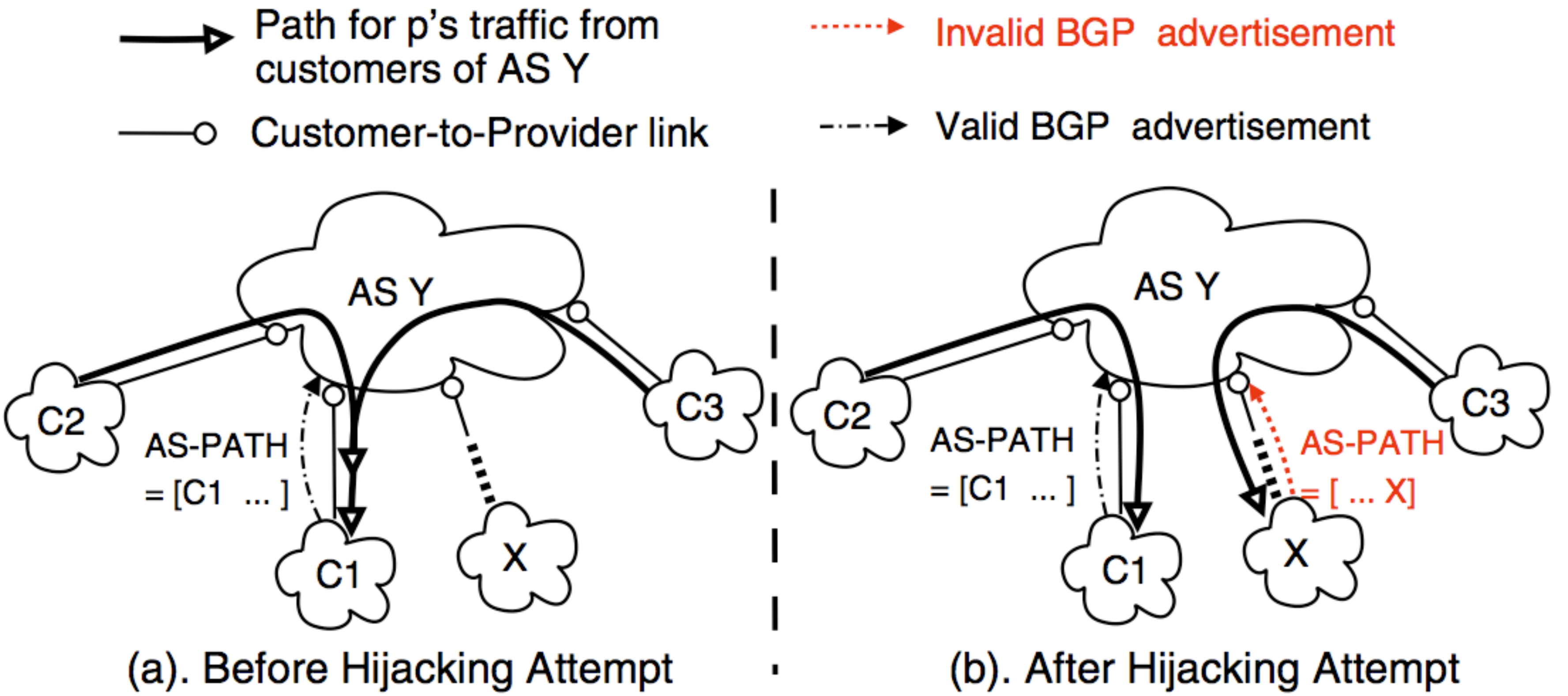


(a). Before Hijacking Attempt

(b). After Hijacking Attempt

Figure 1: AS *Y* has an existing customer-route to *p* and hence, hijacking *p*'s traffic from *Y* with an invalid provider or peer route is not possible.

Partially Successful Hijack

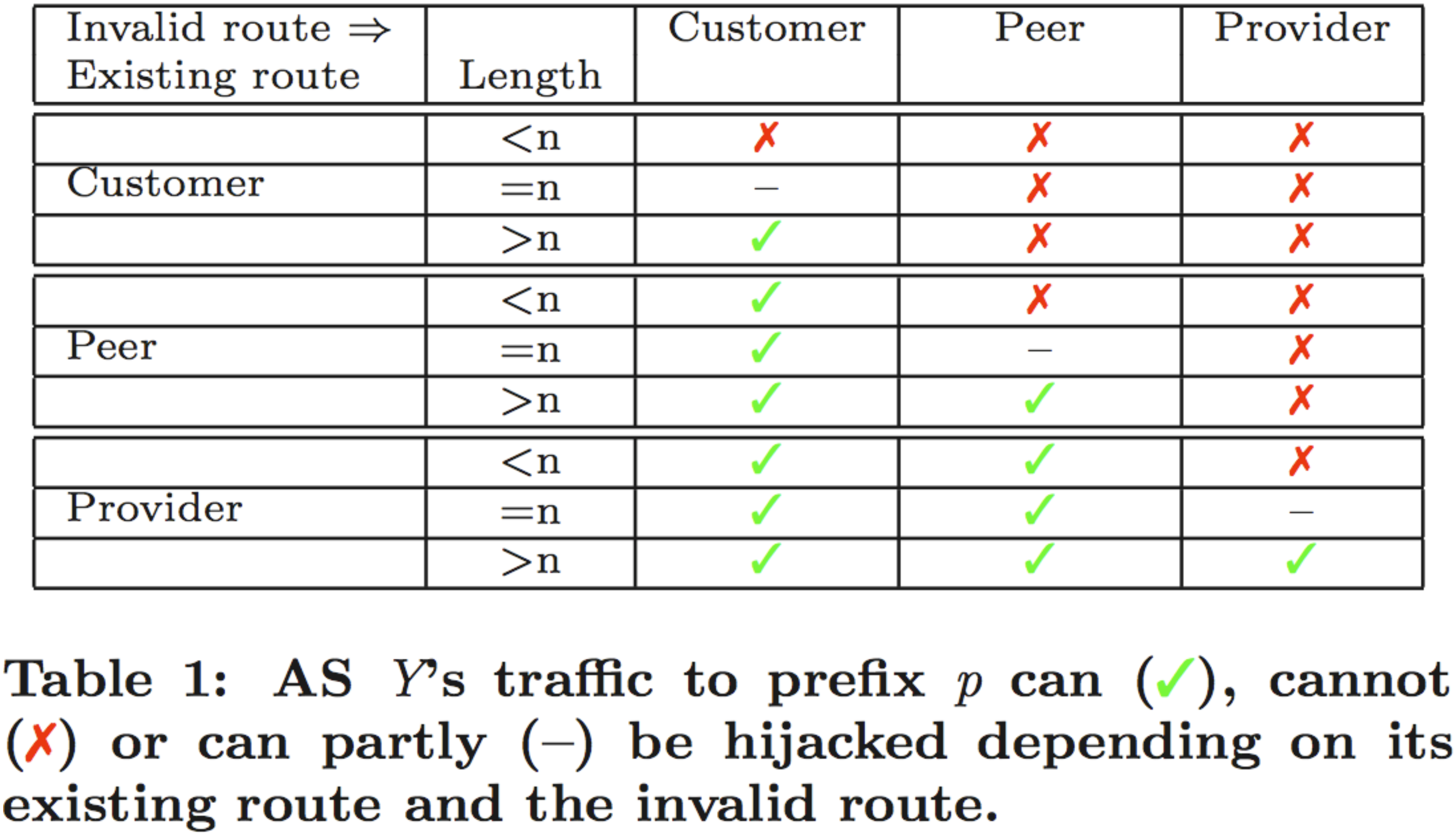


(a). Before Hijacking Attempt

(b). After Hijacking Attempt

Figure 2: AS Y has an existing customer-route to p and receives an invalid route (advertised by AS X) of equal length through a customer. This causes some fraction of p's traffic to be hijacked.

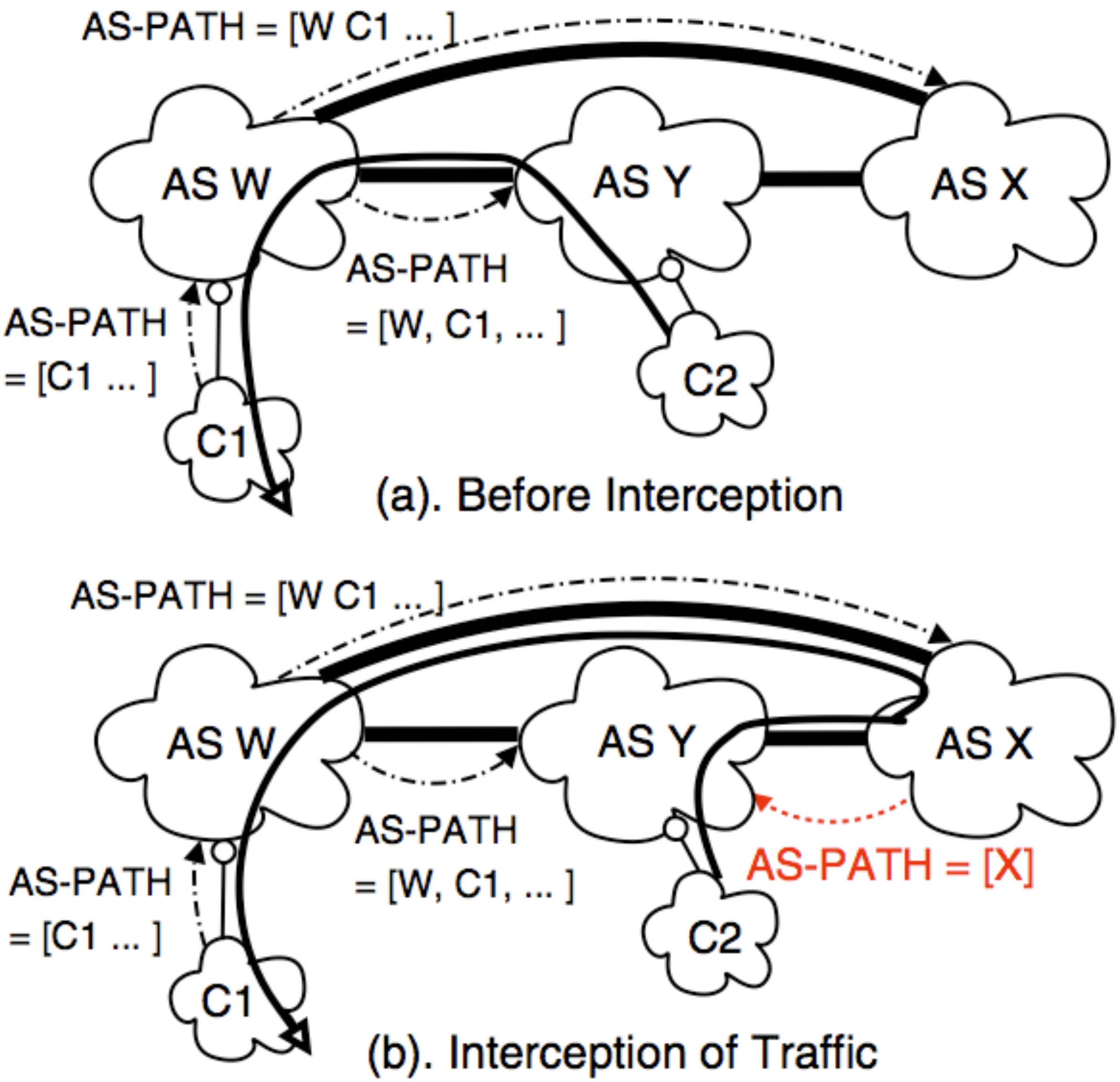
When a hijack will succeed



Invalid route ⇒ Existing route	Length	Customer	Peer	Provider
Customer	<n	✗	✗	✗
	=n	–	✗	✗
	>n	✓	✗	✗
Peer	<n	✓	✗	✗
	=n	✓	–	✗
	>n	✓	✓	✗
Provider	<n	✓	✓	✗
	=n	✓	✓	–
	>n	✓	✓	✓

Table 1: AS *Y*'s traffic to prefix *p* can (✓), cannot (✗) or can partly (–) be hijacked depending on its existing route and the invalid route.

Successful Interception



(a). Before Interception

(b). Interception of Traffic

Unsuccessful Interception

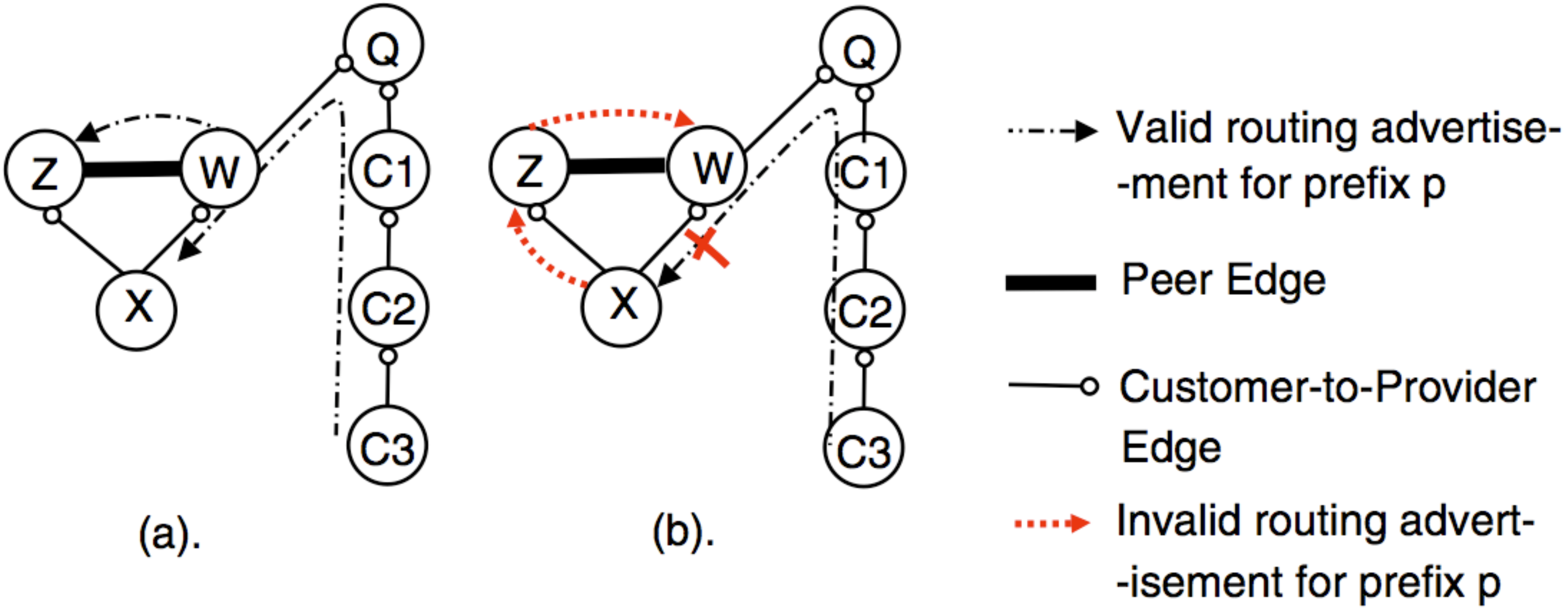


Figure 6: (a) Hijacking AS X has a route for p through provider W. (b) The invalid route advertised by X to another provider Z to intercept p's traffic impacts its existing route for p.

When an interception will succeed

- Goal: deceive all neighbors except the existing next hop to the target prefix.
- If existing route is through a customer or peer, it's safe to announce the false route to other neighbors.
- If existing route is through a provider, it's safe to announce the false route to other peer or customer neighbors.
- Trial-and-error in practice.

The scope of attacks

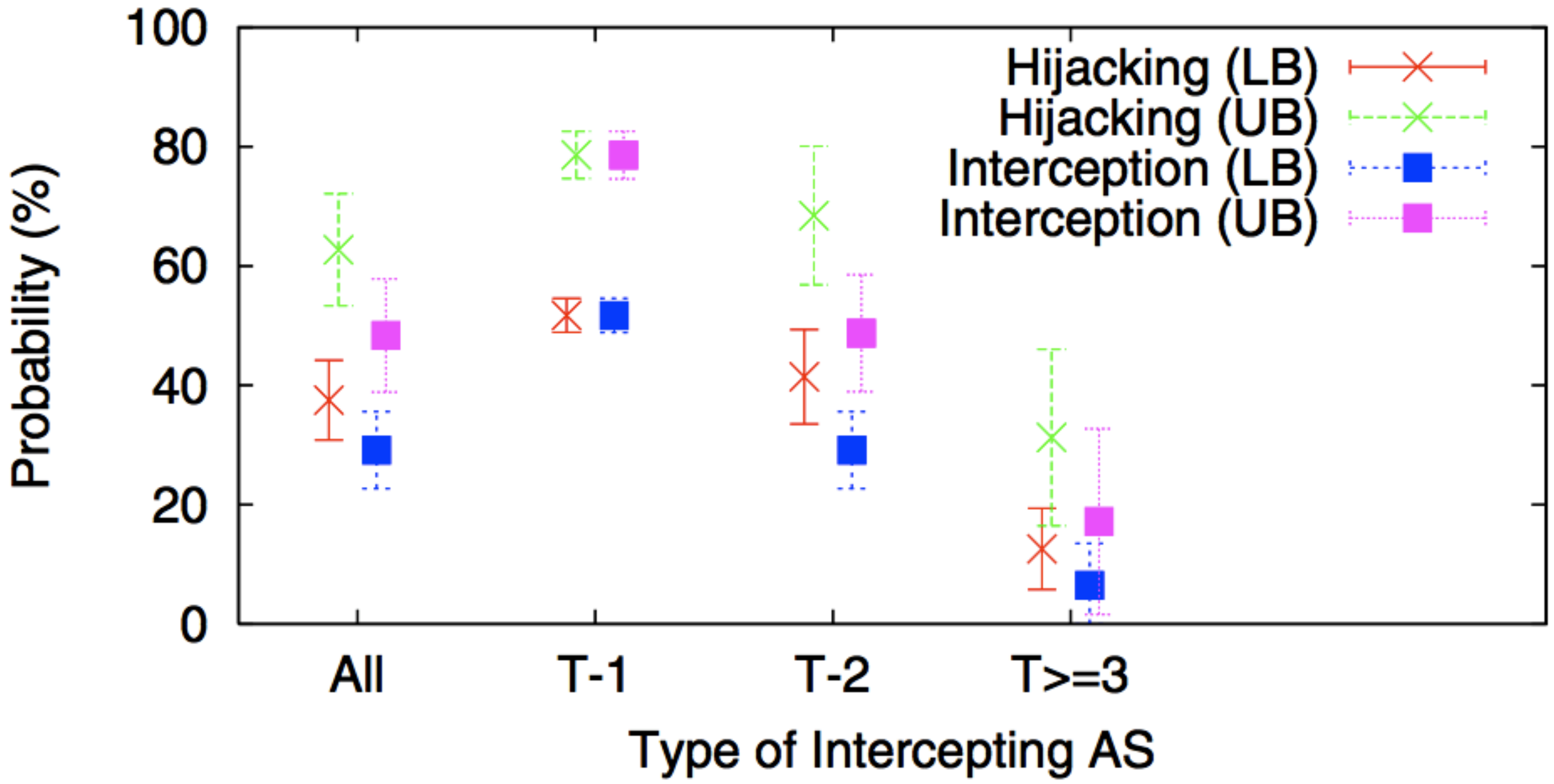


Figure 9: Probability of prefix hijacking and prefix interception for ASes in the RV-set.

Interception Experiment

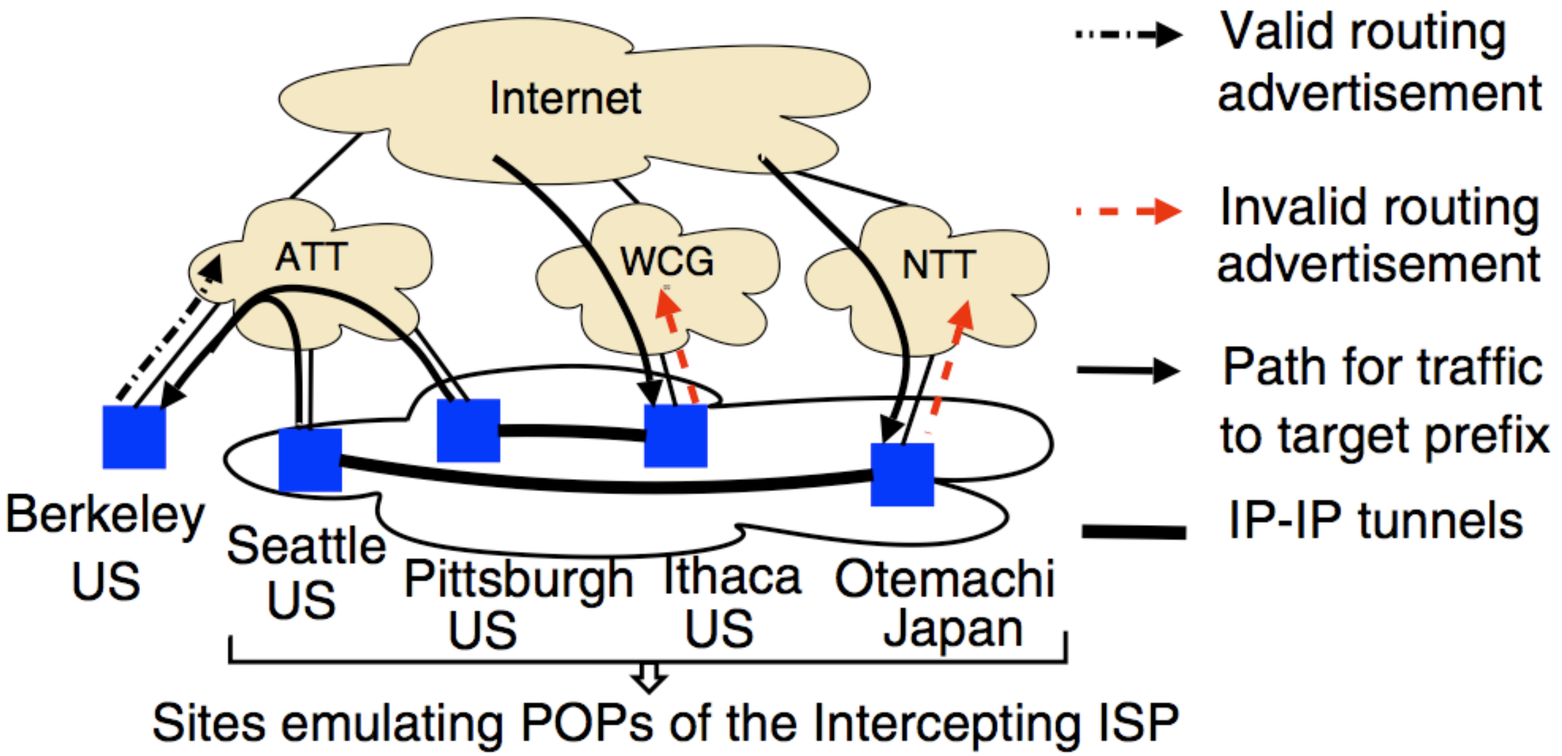
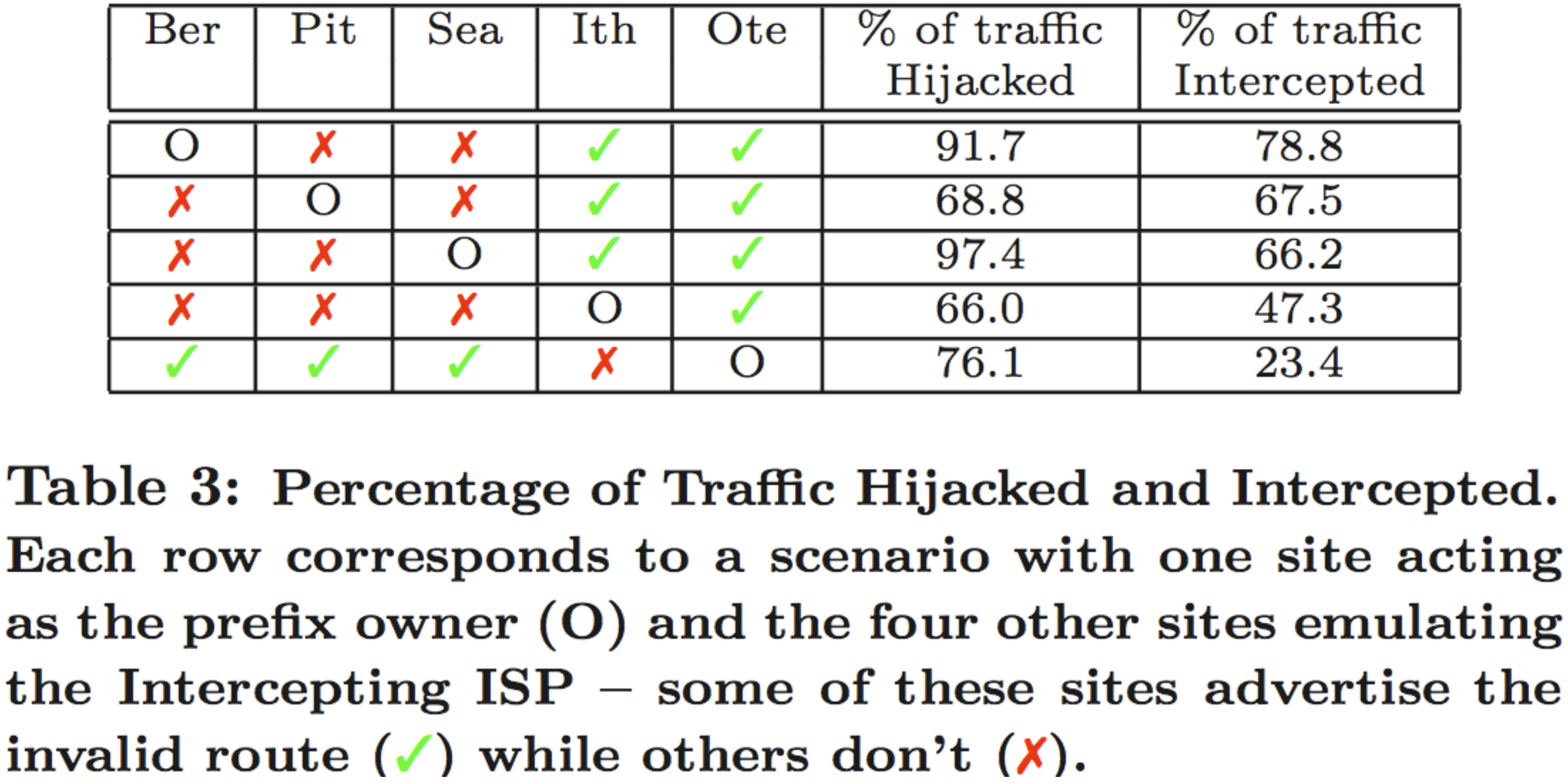

Internet
ATT
WCG
NTT
Berkeley US
Seattle US
Pittsburgh US
Ithaca US
Otemachi Japan
Sites emulating POPs of the Intercepting ISP
Valid routing advertisement
Invalid routing advertisement
Path for traffic to target prefix
IP-IP tunnels

Figure 12: Intercepting traffic from the prefix owner at the Berkeley site. The four other sites emulate an ISP, use invalid routes to hijack traffic and route it back to the owner.

Experiment Result



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

Table 3: Percentage of Traffic Hijacked and Intercepted. Each row corresponds to a scenario with one site acting as the prefix owner (O) and the four other sites emulating the Intercepting ISP – some of these sites advertise the invalid route (✓) while others don't (✗).

Can we detect interceptions?

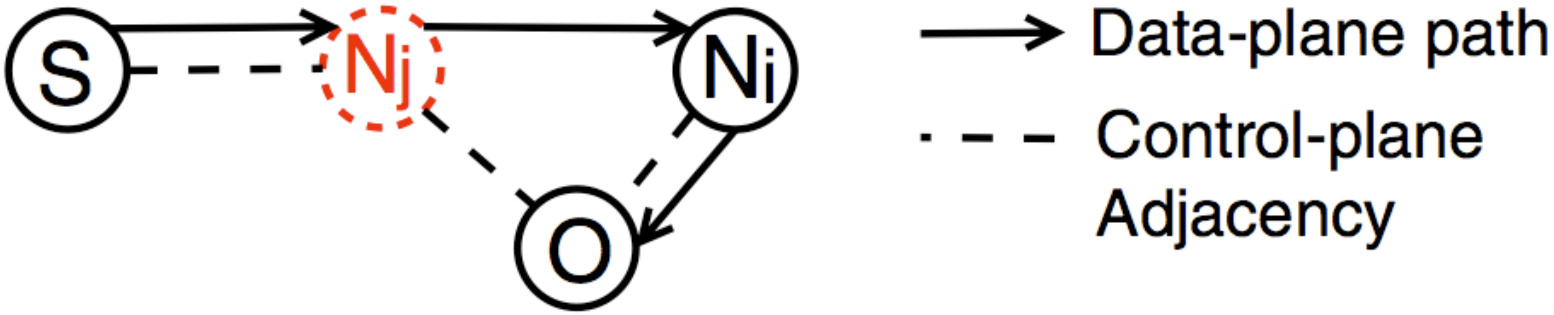
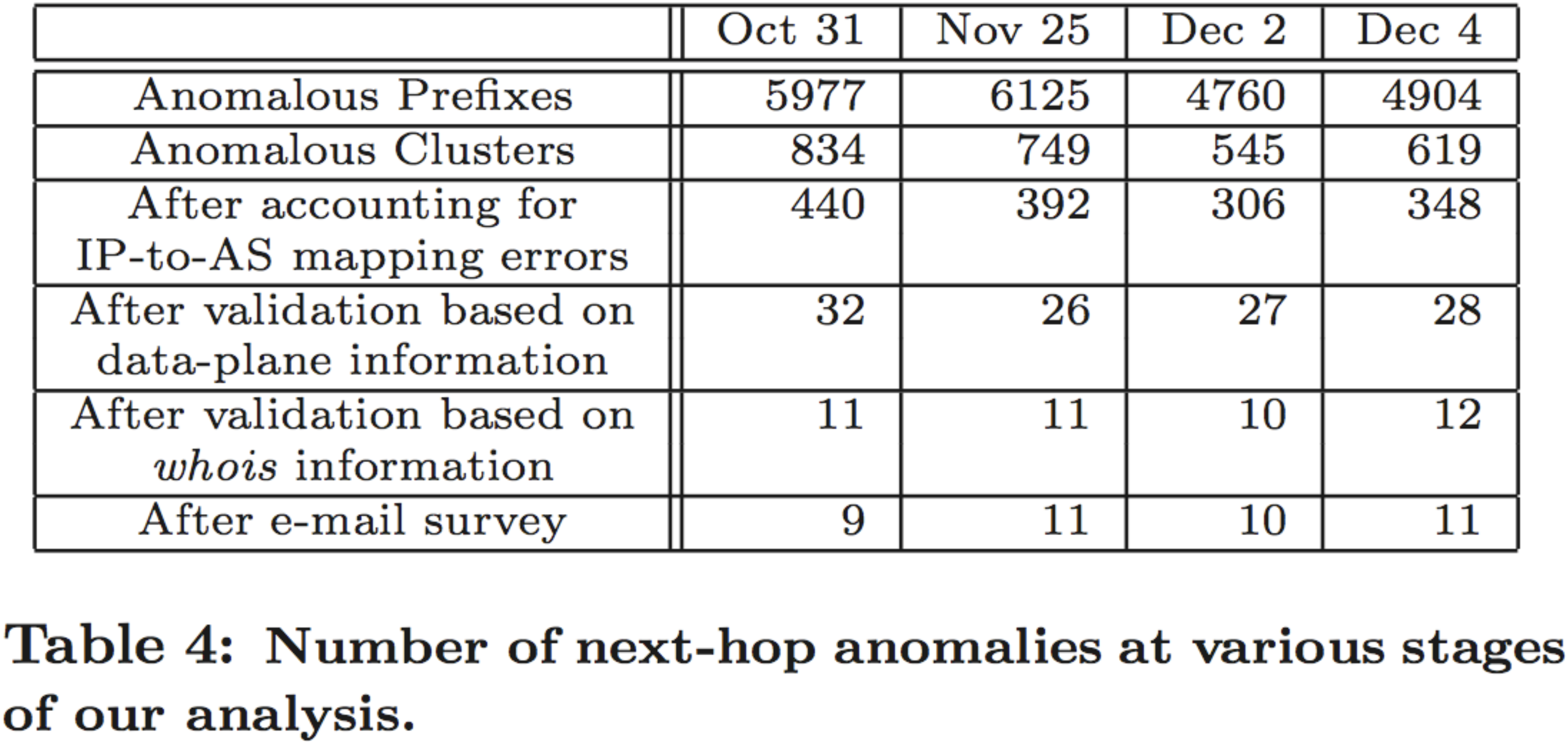


Figure 13: Next-hop Anomaly: a signature for Internet interception. Here, AS N_j uses fake advertisements to claim to be a next-hop for origin AS O and routes intercepted traffic for prefix p through AS N_i.

- If the data path (obtained from traceroute) does not match the announced BGP path, then it might be an interception.

It is very hard



	Oct 31	Nov 25	Dec 2	Dec 4
Anomalous Prefixes	5977	6125	4760	4904
Anomalous Clusters	834	749	545	619
After accounting for IP-to-AS mapping errors	440	392	306	348
After validation based on data-plane information	32	26	27	28
After validation based on *whois* information	11	11	10	12
After e-mail survey	9	11	10	11

Table 4: Number of next-hop anomalies at various stages of our analysis.

- Measurement errors
- Operational practices