



# Understanding impact of prefix hijacks in Internet Routing

Mohit Lad  
UCLA

Ricardo Oliveira  
UCLA

Beichuan Zhang  
Univ. of Arizona

Lixia Zhang  
UCLA

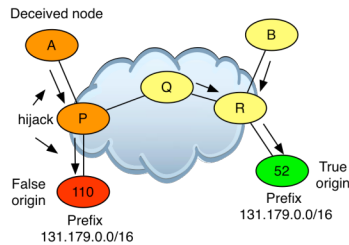
## What is Prefix Hijack?

- Prefix hijack: An autonomous system (AS) announces a prefix it does not own.
  - BGP routers in the Internet might believe this false route and send packets to the false origin.
- Consequence of Prefix hijack
  - Denial of service for true origin and deceived nodes
  - Potential security and privacy breaches
- Entities involved in hijack:
  - True origin: an AS registered to announced the prefix.
  - False origin: an AS announcing a prefix it does not own.
  - Deceived node: an AS believing the route to the false origin.

### Important Questions

- When prefix gets hijacked, what portion of the Internet is deceived?
- What factors influence who gets deceived?
- Which AS nodes can cause most impact as false origins?
- If you plan to connect to Internet, which ISP should you connect to such that
  - If you prefix is hijacked, most nodes will still route to you
  - If other prefixes are hijacked, your routes will still go the true origins

Figure 1



### Aim of our study

- Quantify impact of prefix hijacks and use simulations on Internet scale topology to study impact.
- Identify the primary factor influencing the impact
- Identify characteristics of a node that make it more resilient to prefix hijacks
- Validate analysis and simulation results through case studies involving hijacks from BGP data

## Results:

### Topology and Route Computation

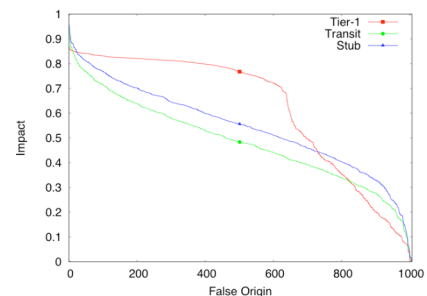
- 22,000 nodes and 60,000 links derived from BGP routing table snapshots and update messages.
- Path selection based on no-valley policy, with preference of route in decreasing order of customer, peer and provider.

### Simulation Setup

- Selected 1000 false origins randomly from a set of 14,000 nodes with unique providers (i.e no two false origins have same connectivity). Added the set of 8 well known tier-1 ISPs as false origins.
- For each false origin, simulated a hijack with every node as a true origin, and measured the impact as the number of nodes believing the false origin.

Figure 2

Impact distribution for true origins belonging to tier-1, transits and stubs.



Tier-1 nodes A,B and C receive a customer route to false origin X, and hence prefer it over peer route to C

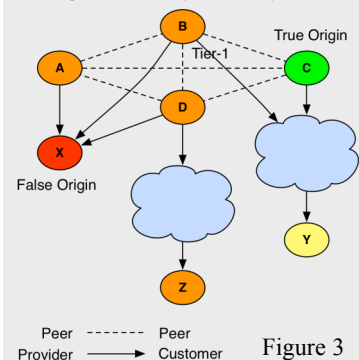


Figure 3

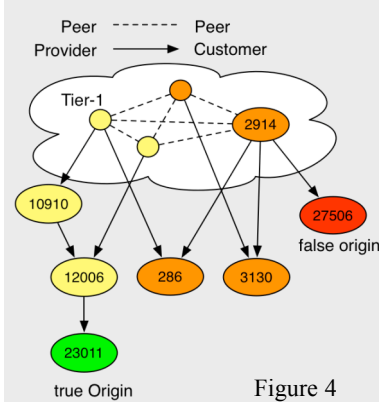


Figure 4

### Spotlight

- Why are Tier-1's more vulnerable than transits?
- Which nodes have highest impact?
- Which nodes are most vulnerable?

### How to cause high impact?

- Tier-1 nodes and large ISPs have huge customer base.
- If false origin deceives tier-1 node, then good chance of deceiving customers, and cause high impact.

### How to deceive tier-1?

- Tier-1 nodes use peer routes between each other
- If a tier-1 node receives a competing customer route from false origin, it will be deceived, since customer route is more preferred than peer route.

### Hijacking tier-1 node

- If true origin is a tier-1, then all tier-1 nodes on the provider path of false origin will be deceived. See Figure 3 explaining simulation results.

### High impact false origin

- False origin reaching many tier-1 nodes in short hops causes high impact in most cases.

### Case study

- AS 27506 announced routes belonging to over 20 different AS nodes. Figure 4 shows how impact increases when true origin is farther away from tier-1 compared to the false origin.

### Summary

Connecting to multiple tier-1's increases resiliency against prefix hijacks.

A tier-1 node is vulnerable to hijacks, since other tier-1 nodes would prefer a customer route from the false origin.