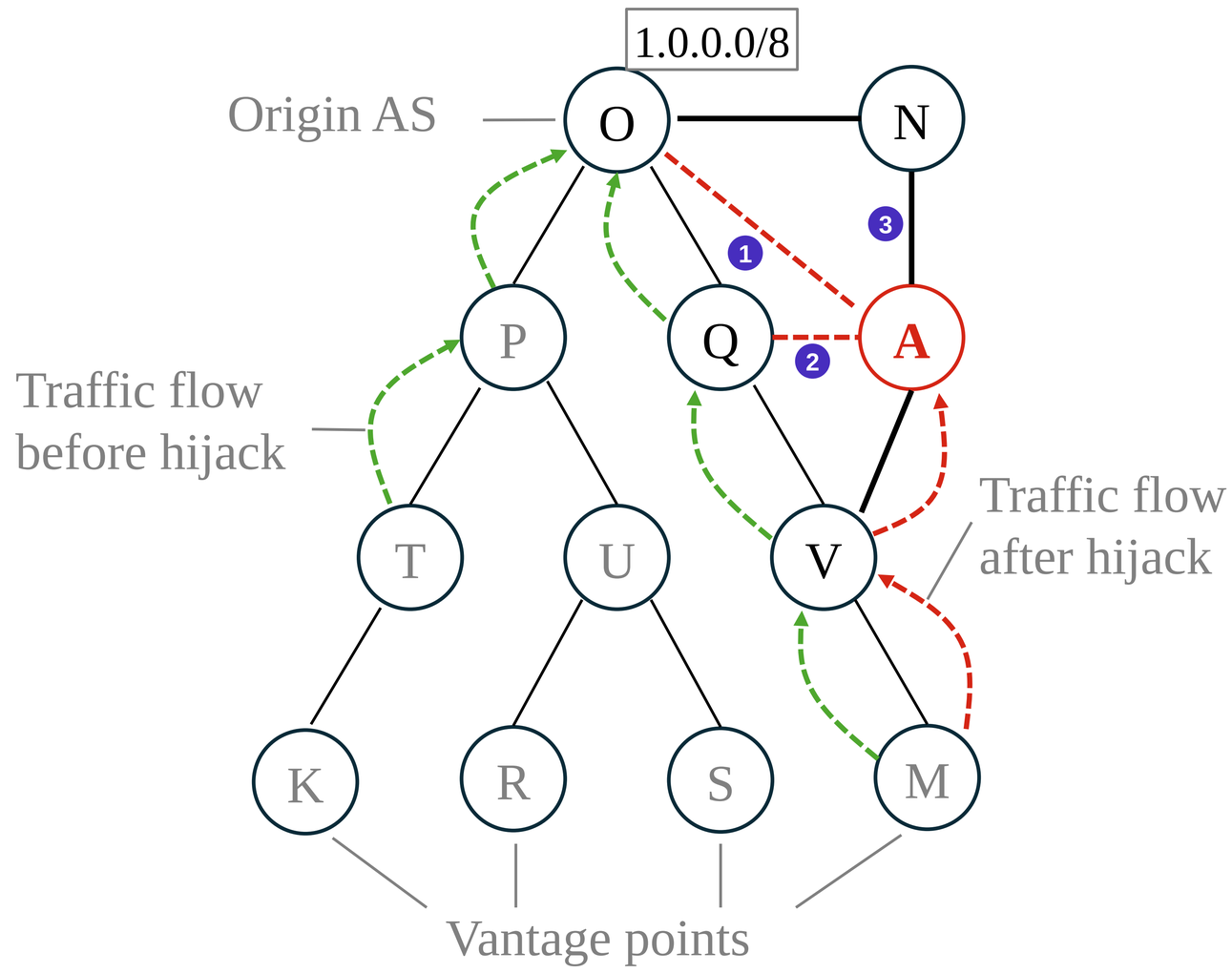
Adaptive Evasion of Tree-Based BGP Path Hijacking Detectors

Ilias Chanis, Shahrooz Pouryousef, Muoi Tran

RQ: Can an adaptive adversary evade a tree-based BGP hijack detector by forging routing trees that look benign?



Ares[1]: the state-of-the-art hijack detector

Clusters the routing trees that collectors see for each prefix.
Alarms when a new tree won't merge and its edges are invalid.

Does Ares detect it?

1 Naive hijack · A–O — ✗ detected

Adds a fake link directly to the origin,
so a new tree appears that will not merge.

2 Tree manipulation · A–Q–O — ✓ evades

Grafts the fake link deeper in an existing branch,
so the new tree stays within Ares's merge threshold.

3 Heuristic bypass · A–N–O — ✓ evades

Uses only real, valley-free edges, so it
passes Ares's path-validity heuristic.

Dataset: 13 historical BGP hijacks[2] (2008–2016) · **Simulation:** Gao–Rexford propagation on the CAIDA AS-graph[3]
Success = an announcement that both evades Ares and reroutes ASes through the attacker

Evasion on 13 historical hijacks (2008–2016)

Event	Threshold	Heuristic	Switched	Disrupted
defcon_1	✓	✓	503	1,399
facebook_1	✓	✓	4	1,203
france_1	✓	✓	62	1,760
torg_1	✗	✗	–	–
torg_2	✗	✗	–	–
petersburg_1	✓	✓	453	562
petersburg_2	✓	✓	453	562
bitcanal_3	✓	✓	1	622
bitcanal_4	✓	✓	1	622
enzu_1	✓	✗	2	**2,441**
backconnect_3	✓	✗	1	161
backconnect_6	✓	✗	1	9
typo_1	✗	✗	–	–

10 / 13
evade via tree manipulation

7 / 13
via heuristic bypass

4.9%
of ASes rerouted
up to 2,441 (enzu_1)

Tree manipulation wins

- Evades every event heuristic bypass does, plus three others.
- Grafting the fake link deeper down the tree trades impact for stealth.

One AS can be enough

- enzu_1: two ASes take the forged route, one is **AS174 (Cogent, Tier-1)**.
- A single well-placed AS leads to major disruption (facebook_1, bitcanal_3).

What limits the attacks

- Valley-free export limits reach to the attacker's customer cone.
- Shallow trees expose the forged route, pushing it past the threshold.

Adaptive adversaries can evade detectors built on public routing data.

Why it matters: The attacker sees the same public data as the detector, so it can make a malicious change look benign.

Next: Robust detection needs signals the adversary cannot easily control, such as data-plane measurements.

References

1. Y. Tao et al. Comprehensive Path Hijacking Detection via Routing Tree. USENIX Security 2025.
2. S. Cho et al. BGP Hijacking Classification. IEEE TMA 2019.
3. M. Luckie et al. AS Relationships, Customer Cones, and Validation. ACM IMC 2013.

Acknowledgments: partially supported by WASP, funded by the Knut and Alice Wallenberg Foundation.

Read the paper
doi.org/10.1145/3830454.3846444
Contact: chanis@chalmers.se