# Understanding the Stealthy BGP Hijacking Risks in the ROV Era

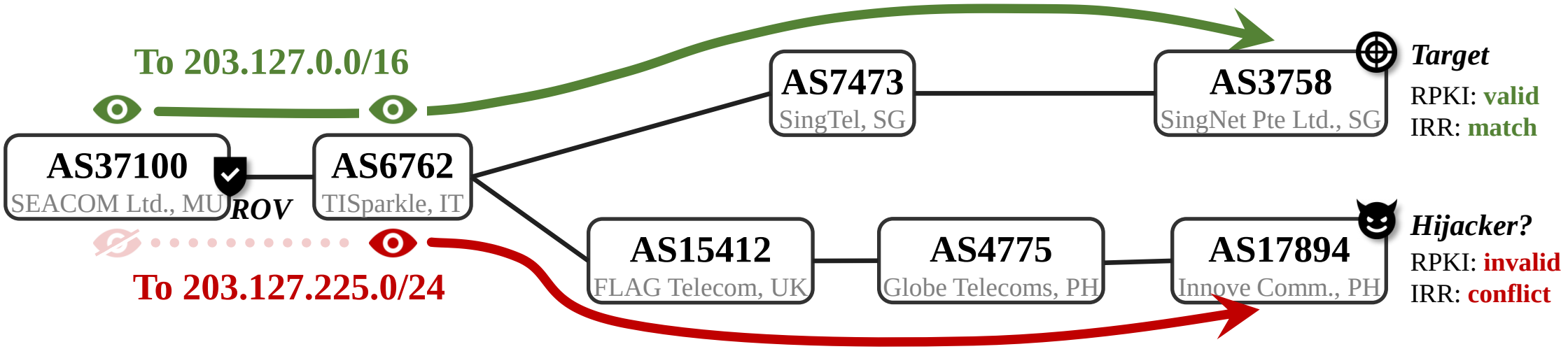
Yihao Chen, Qi Li, Ke Xu, Zhuotao Liu, Jianping Wu

Tsinghua University

# Content

1. BGP Hijacking in the ROV Era: A Real-World Case
2. Stealthy BGP Hijacking
3. Empirical Analysis & Insights
4. Simulation-Based Risk Evaluation
5. Discussion & Future Work

# BGP Hijacking in the ROV Era: A Real-World Case




* First observed: 2023-10-01 Recently observed: 2025-02-05
* While in the form of BGP hijacking, this case is very likely to be caused by misconfiguration; we awaiting response from relevant operators.

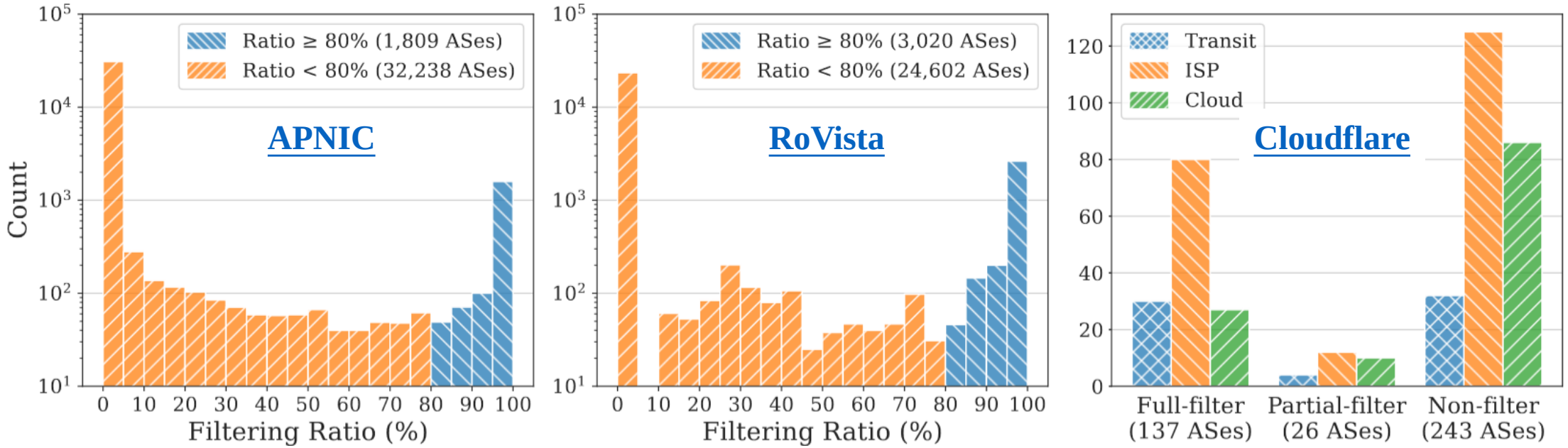
- AS17894 mis-announces a /24 without RPKI or IRR authorization, while AS3758 is the legitimate origin
- ROV-enabled AS37100 discards the invalid route, and thus **has the legitimate /16 route only**

  → By seeing routing tables, AS37100 and its customers are **not aware of the potential hijacking attempt**, and tend to believe their traffic be forwarded correctly.
- However, **legacy AS6762 accepts the illegitimate route**, actually forwarding /24 traffic to AS17894

**BGP hijacking still succeeds, and becomes less spotted (stealthier), due to the incomplete ROV deployment in the current Internet?**

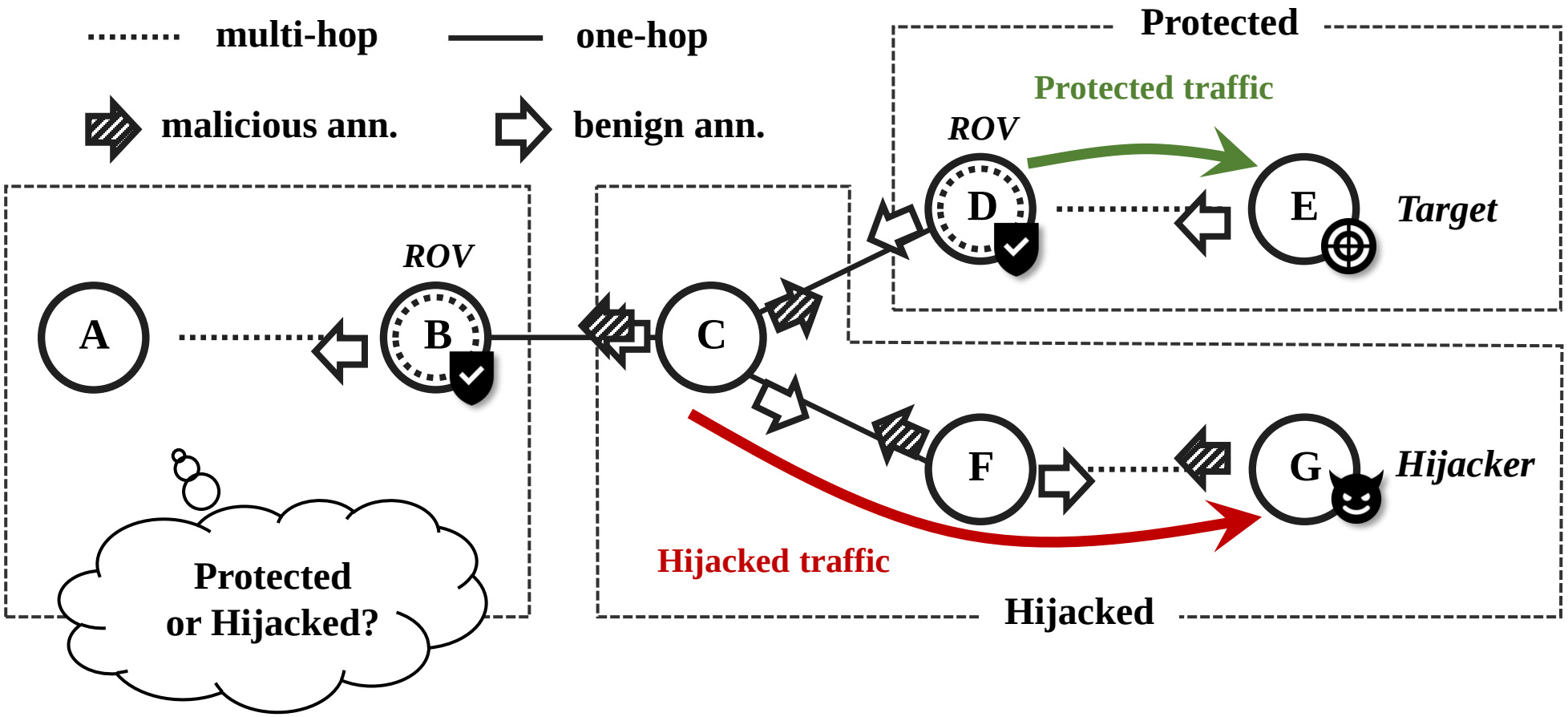
# RPKI/ROV in Today's Internet

- ROAs have covered **53.9% IPv4 prefixes** and **59.2% IPv6 prefixes***
- Yet ROV deployment is **presumably limited**



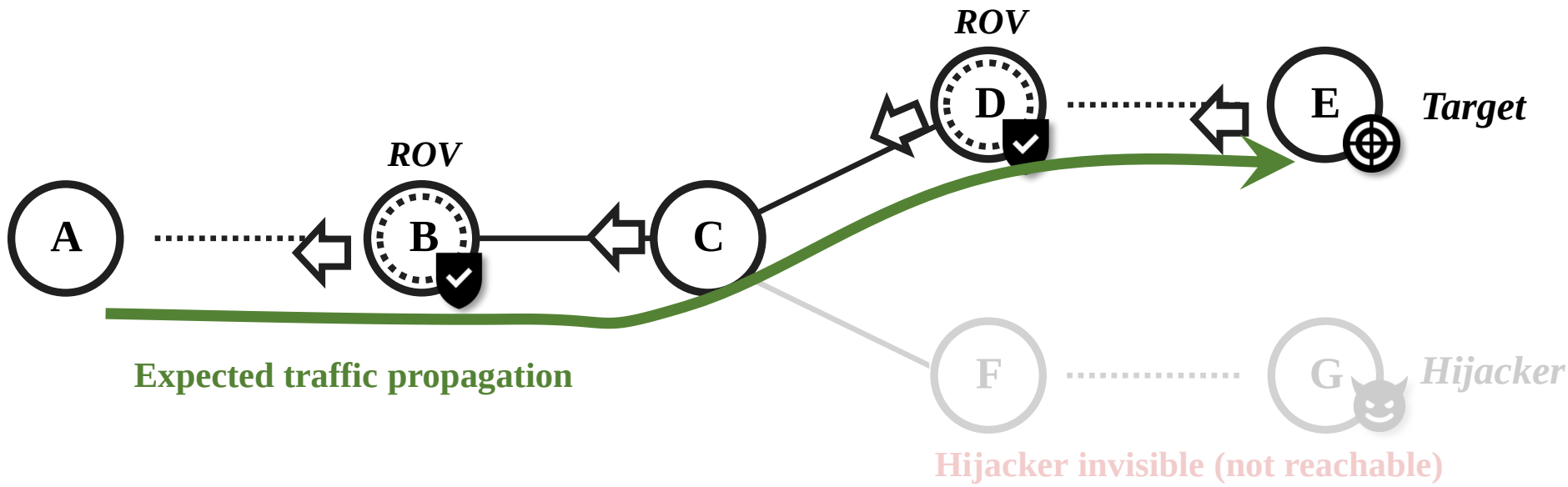

* Source: https://rpki-monitor.antd.nist.gov/ROV

# BGP Hijacking Under Partial ROV deployment



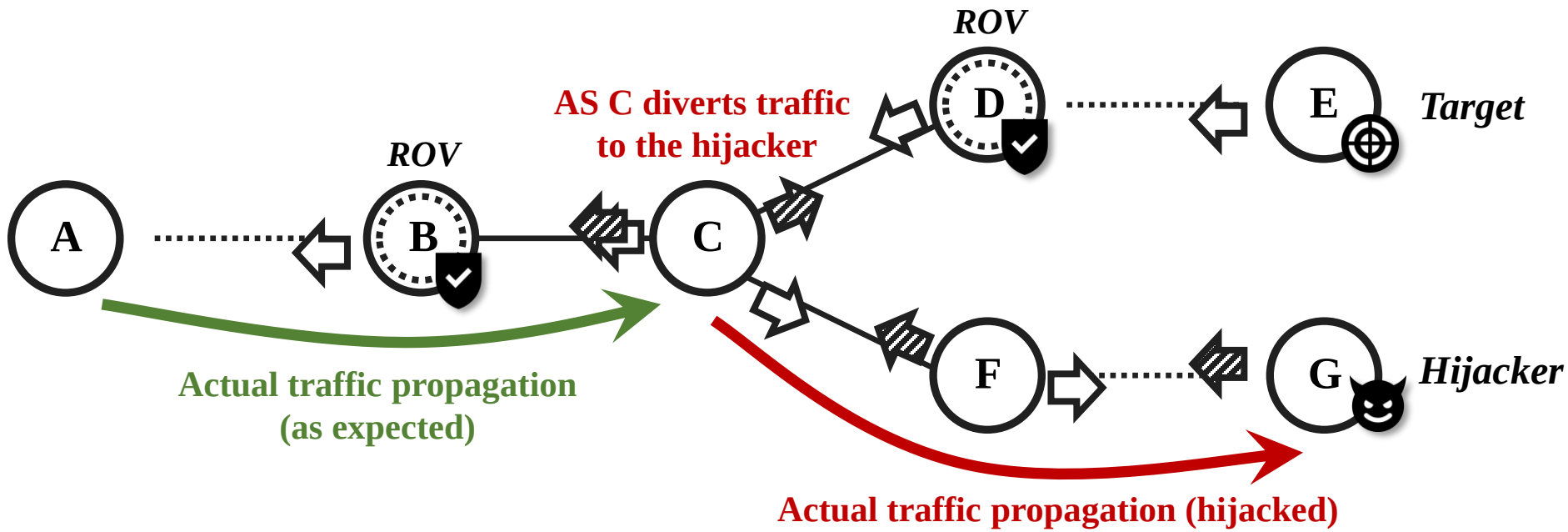

* This is the general topology structure that illustrates how BGP hijacking could succeed despite partial ROV deployment. It does not reflect the whole Inter-AS topology, but only the part that makes the stealthy hijacking scenario possible.

# AS A's Perspective



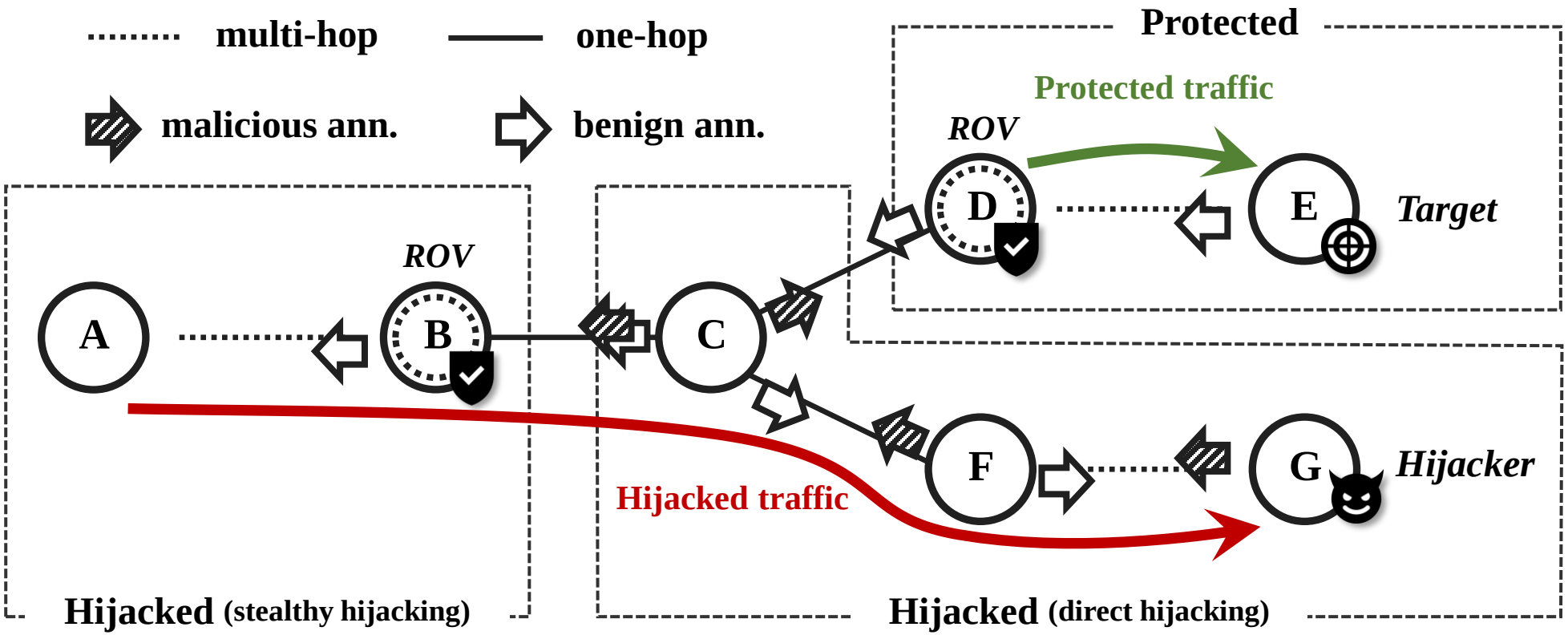

- The hijacker is invisible to AS A on the control plane, due to the ROV filtering of AS B
- AS A would expect its traffic safely forwarded along the correct path (green)

# Global Perspective




- AS C, however, is not protected by ROV, and diverts traffic to the hijacker, as long as it accepts the prefix (either the target prefix or a subprefix of it) announced by the hijacker.
- AS A falls victim to hijacking unknowingly.

# Stealthy Hijacking: An Unexpected Consequence




BGP hijacking that is invisible from the victim on the control plane

# Empirical Analysis of Stealthy Hijacking in the Wild

## Data Sources

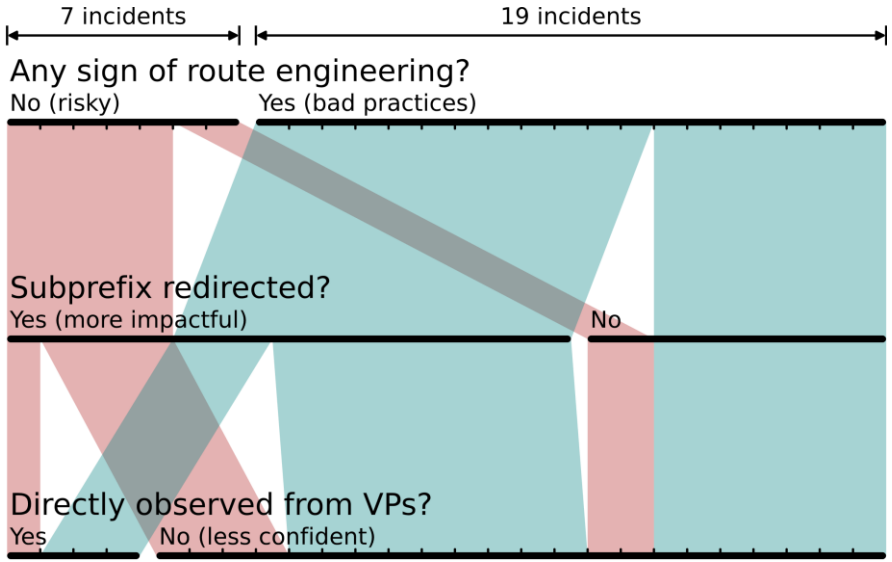
- RIB data from RouteViews collectors (route-views2, amsix, wide) on Oct 1, 2023 (56M routes, 86 vantage points).
- Validation: RIPE NCC RPKI, RADB IRR, WHOIS from 5 RIRs, CAIDA AS Organization dataset..

## Results

- **26 incidents**: 19 linked to poor route engineering (e.g., outdated RPKI/IRR), 7 potential hijacks.
- **Affected:** 1,205 routes, 40 prefixes, 27 origins.

| Type | #Prefixes | #Origins | #Routes | #VPs |
|---|---|---|---|---|
| Risky incidents | 10 | 7 | 120 | 45 |
| Bad practices | 30 | 20 | 1,085 | 57 |
| Total | 40 | 27 | 1,205 | 57 |

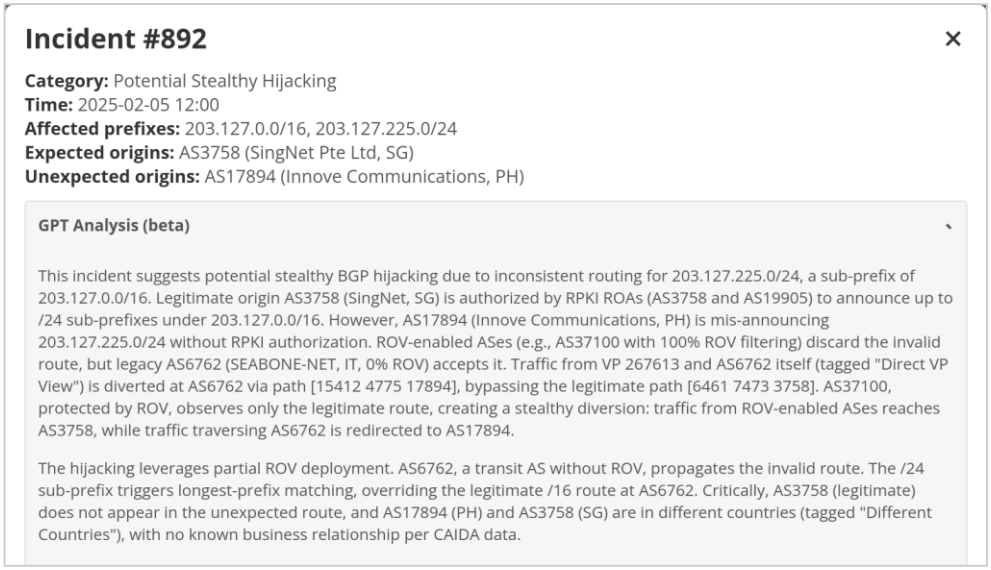
**#0 Most wild stealthy hijacking is caused by bad route engineering practice.**

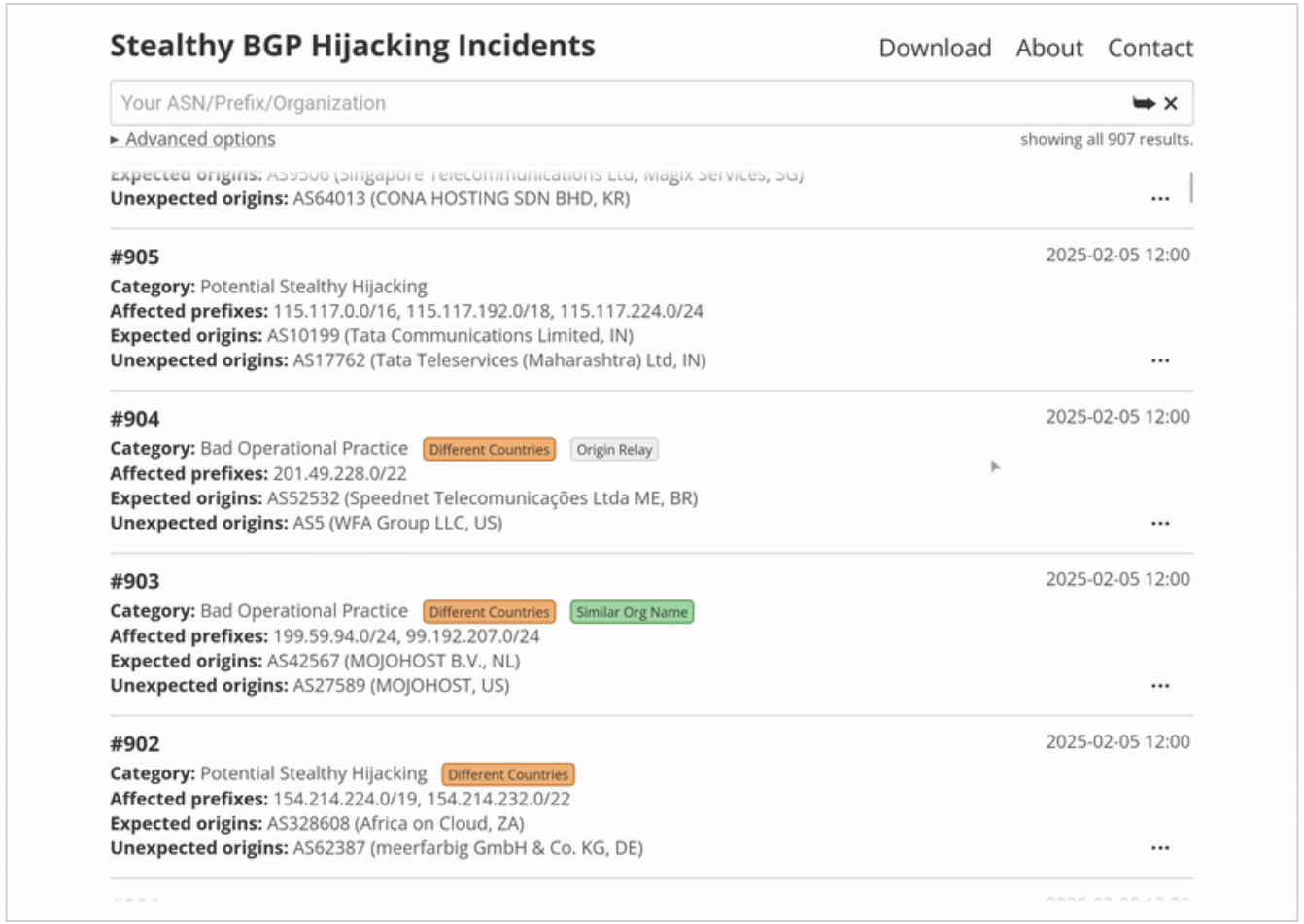


# Empirical Analysis: Public Service

Our website to publish stealthy hijacking incidents in the wild: https://yhchen.cn/stealthy-bgp-hijacking/

- Set up search options and date range
- Search your interested ASN/prefix/organization
- Review the results and feedback
- Beta feature: GPT analysis with routing knowledge augmentation




* Daily analysis results since 2025-01-01

# Simulation-Based Risk Evaluation

**Questions unanswered:**

The prevalence, extent, distribution, influencing factors, etc. of the risk within our real-world Internet.

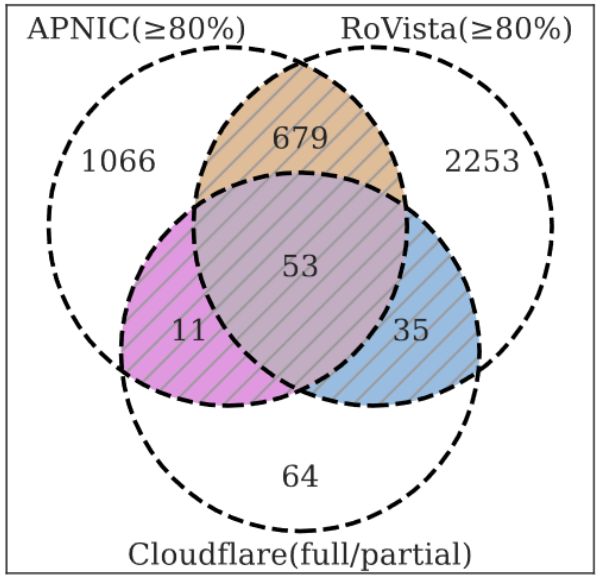
- Use **CAIDA AS relationships** to reconstruct Internet topology
- Use **APNIC, RoVista, Cloudflare** measurement to gain ROV deployment status
- Perform BGP simulation on the topology and generate **all Internet-scale routes**
- Thoroughly analyze **all possible "victim-target-hijacker" 3-tuple** to determine those at risk of stealthy BGP hijacking.

Is it possible to **comprehensively** evaluate the stealthy hijacking risk introduced by the **current** ROV deployment?

**Challenges: Criteria to identify risk? Knowledge of routes?**

**Measurement of ROV deployment? .....**

# Results: Overall Risk Level



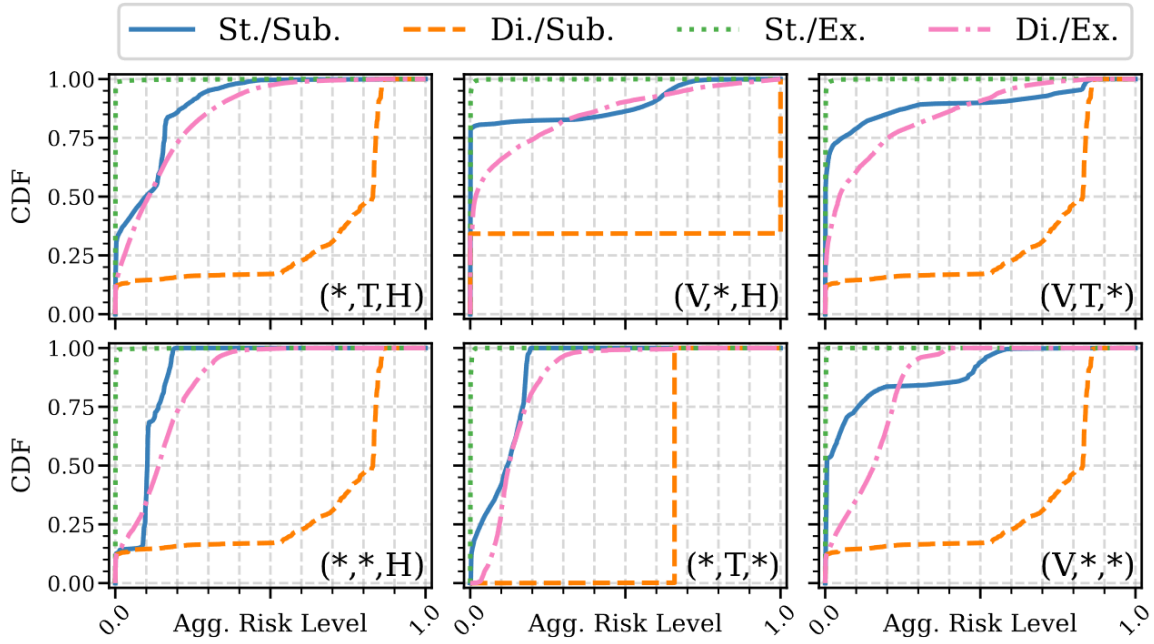
778 ASes identified ROV-enabled by at least two sources

| **Stealthy Hijacking** | Sub-Prefix | Exact-Prefix |
|---|---|---|
| w/ ROV | 0.104 ▲0.104 | 0.001 ▲0.001 |
| w/o ROV | 0.000 | 0.000 |

| **Direct Hijacking** | Sub-Prefix | Exact-Prefix |
|---|---|---|
| w/ ROV | 0.658 ▼0.328 | 0.144 ▼0.194 |
| w/o ROV | 0.986 | 0.338 |

**#1** The overall success rate of stealthy hijacking increases from 0 to 10.4%, solely due to the partial ROV deployment in today's Internet.

# Results: Aggregated Risk Level

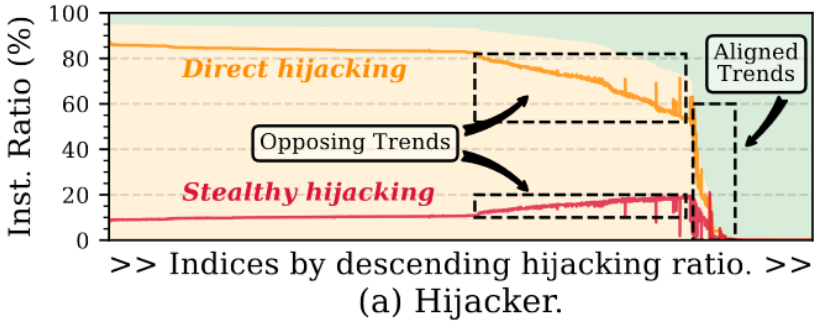


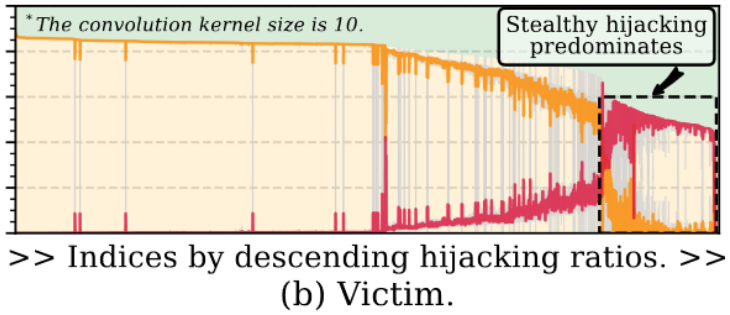

**#2** Targeted stealthy hijacking has high success rates on specific AS pairs (up to 99.5%), while non-targeted one spreads risk more evenly (within 21.0%).

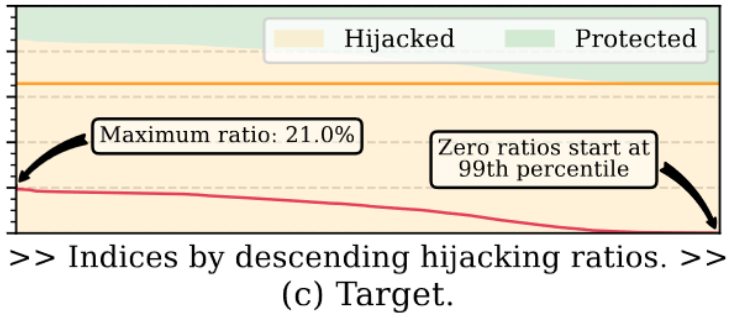
| Statistics[1] | | Hijacking Type[2] St./Sub. | Di./Sub. | St./Ex. | Di./Ex. |
|---|---|---|---|---|---|
| $\mathcal{P}$(*,T,H) | *min* | 0.000▼0.000 | 0.000▼0.000 | 0.000▼0.000 | 0.000▼0.000 |
| | *25th* | 0.003▲0.003 | 0.629▼0.362 | 0.000▼0.000 | 0.029▼0.132 |
| | *50th* | 0.096▲0.096 | 0.830▼0.164 | 0.000▼0.000 | 0.108▼0.176 |
| | *75th* | 0.159▲0.159 | 0.840▼0.154 | 0.000▼0.000 | 0.212▼0.280 |
| | *max* | 0.995▲0.995 | 0.880▼0.116 | 0.990▲0.990 | 0.880▼0.116 |
| $\mathcal{P}$(V,*,H) | *min* | 0.000▼0.000 | 0.000▼0.000 | 0.000▼0.000 | 0.000▼0.000 |
| | *25th* | 0.000▼0.000 | 0.000▼1.000 | 0.000▼0.000 | 0.000▼0.116 |
| | *50th* | 0.000▼0.000 | 1.000▼0.000 | 0.000▼0.000 | 0.018▼0.252 |
| | *75th* | 0.000▼0.000 | 1.000▼0.000 | 0.000▼0.000 | 0.211▼0.307 |
| | *max* | 0.995▲0.995 | 1.000▼0.000 | 0.994▲0.994 | 1.000▼0.000 |
| $\mathcal{P}$(V,T,*) | *min* | 0.000▼0.000 | 0.000▼0.000 | 0.000▼0.000 | 0.000▼0.000 |
| | *25th* | 0.000▲0.000 | 0.629▼0.362 | 0.000▼0.000 | 0.005▼0.061 |
| | *50th* | 0.000▲0.000 | 0.830▼0.164 | 0.000▲0.000 | 0.046▼0.208 |
| | *75th* | 0.055▲0.055 | 0.840▼0.154 | 0.001▲0.001 | 0.201▼0.382 |
| | *max* | 0.877▲0.877 | 0.880▼0.116 | 0.347▲0.347 | 0.880▼0.116 |
| $\mathcal{P}$(*,*,H) | *min* | 0.000▼0.000 | 0.000▼0.000 | 0.000▼0.000 | 0.000▼0.000 |
| | *25th* | 0.096▲0.096 | 0.629▼0.362 | 0.000▲0.000 | 0.067▼0.172 |
| | *50th* | 0.103▲0.103 | 0.830▼0.164 | 0.000▲0.000 | 0.139▼0.184 |
| | *75th* | 0.139▲0.139 | 0.840▼0.154 | 0.001▲0.001 | 0.209▼0.220 |
| | *max* | 0.210▲0.210 | 0.880▼0.116 | 0.425▲0.425 | 0.710▼0.175 |
| $\mathcal{P}$(*,T,*) | *min* | 0.000▼0.000 | 0.658▼0.328 | 0.000▼0.000 | 0.011▼0.011 |
| | *25th* | 0.034▲0.034 | 0.658▼0.328 | 0.000▲0.000 | 0.094▼0.122 |
| | *50th* | 0.120▲0.120 | 0.658▼0.328 | 0.001▲0.001 | 0.124▼0.183 |
| | *75th* | 0.170▲0.170 | 0.658▼0.328 | 0.001▲0.001 | 0.179▼0.248 |
| | *max* | 0.210▲0.210 | 0.658▼0.328 | 0.045▲0.045 | 0.658▼0.328 |
| $\mathcal{P}$(V,*,*) | *min* | 0.000▼0.000 | 0.000▼0.000 | 0.000▼0.000 | 0.000▼0.000 |
| | *25th* | 0.002▲0.002 | 0.629▼0.362 | 0.000▲0.000 | 0.052▼0.247 |
| | *50th* | 0.005▲0.005 | 0.830▼0.164 | 0.001▲0.001 | 0.157▼0.174 |
| | *75th* | 0.106▲0.106 | 0.840▼0.154 | 0.002▲0.002 | 0.218▼0.164 |
| | *max* | 0.854▲0.854 | 0.880▼0.116 | 0.031▲0.031 | 0.408▼0.049 |
| $\mathcal{P}$(*,*,*) | — | 0.104▲0.104 | 0.658▼0.328 | 0.001▲0.001 | 0.144▼0.194 |

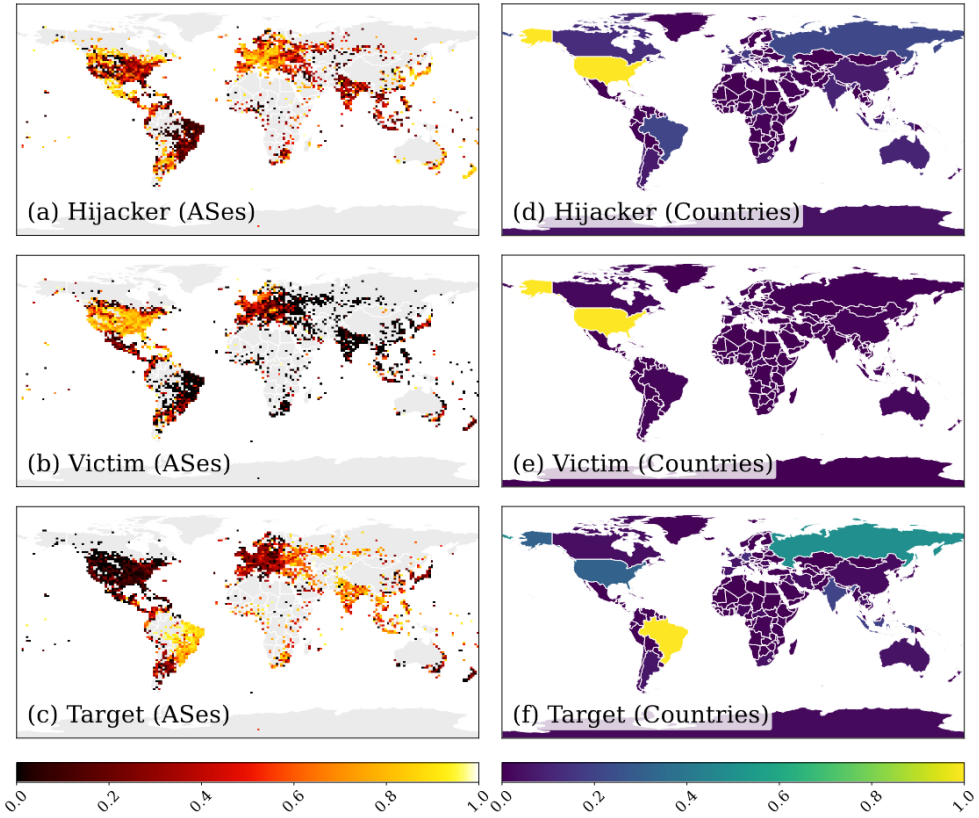
[1] *25th*, *50th*, and *75th* represent the respective percentiles.
[2] St., Di., Sub., and Ex. stand for "stealthy", "direct", "sub-prefix", and "exact-prefix". The difference (▼/▲) is based on the comparison with no AS deploying ROV.

# Results: Risk Distribution



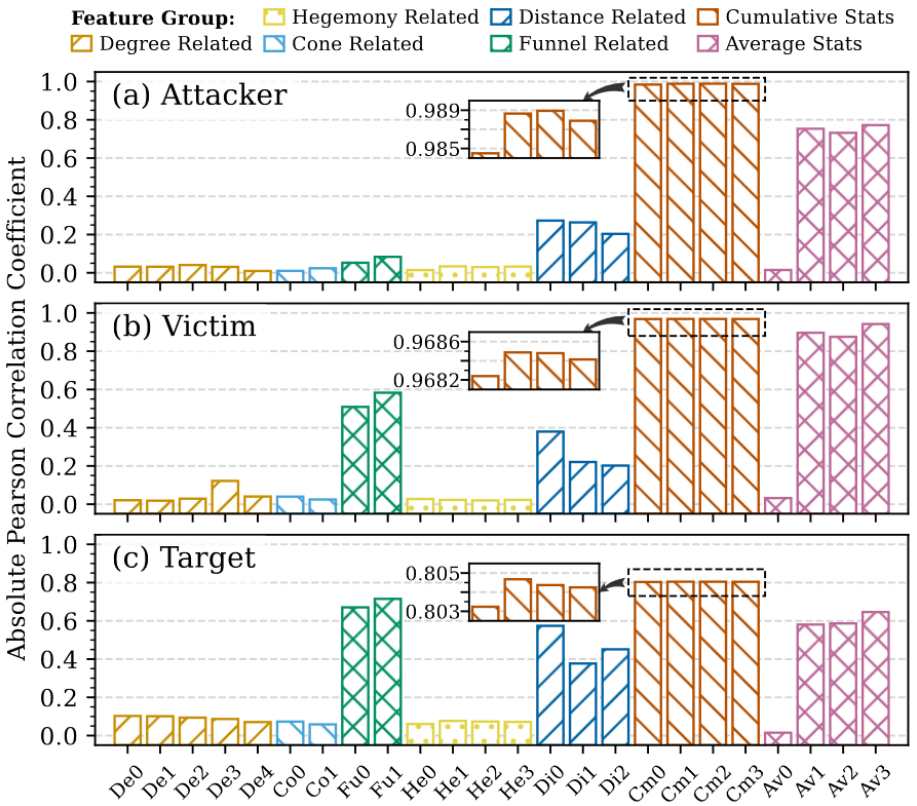



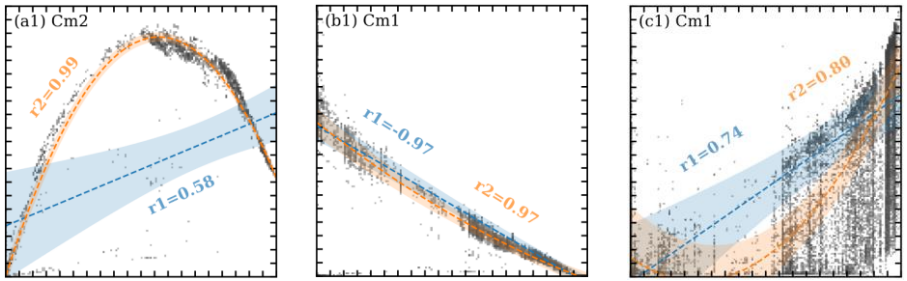



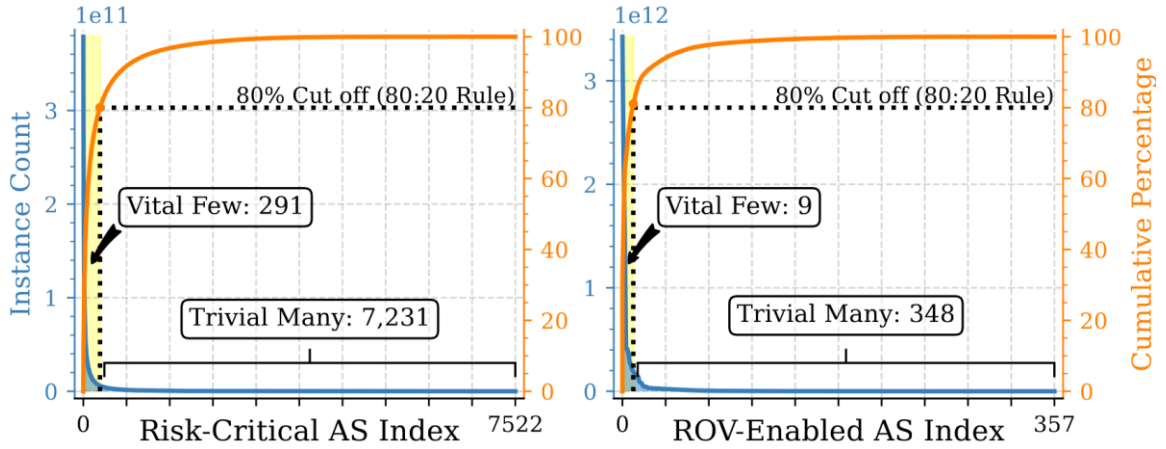

**#3** Stealthy hijacking risks typically follow an opposing trend to direct hijacking as ROV's impact increases.

**#4** Arguably, ASes most capable of hijacking are mainly in Europe and parts of North America. Victim-prone ASes are mainly in North America. Target-prone ASes are mainly in South America and South Asia.

# Results: Influencing Factors




**#5** Among different features, cumulative statistics of AS hegemony exhibit highest quadratic correlation with the risk.

**#6** A small set of risk-critical and ROV-enabled ASes account for the majority of stealthy hijacking risk.

# Discussion & Future Work

**Limitations of the approach**

- Prefix-specific routing simulation?
- Accuracy-coverage trade-off of ROV cross validation?
- Complex routing policy?

**Potential practical application**

- For ISP operation: risk assessment before peering plans
- To defend attacks: targeted probing, analysis with real-world routes, ……

**Risk countermeasures**

- Keep increasing RPKI/ROV deployment (as indicated in #3)
- Co-analyzing routing data from multiple VP to identify inconsistencies
- Collaboration among ROV-enabled ASes to share threat information
- Active blackholing on detecting stealthy hijacking (like in ROV++)

# Summary

## **Motivation:** a real-world case

BGP Hijacking in the ROV Era: A Real-World Case




* First observed: 2023-10-01. Recently observed: 2025-02-05
* While in the form of BGP hijacking, this case is very likely to be caused by misconfiguration; we awaiting response from relevant operators.

- AS17894 mis-announces a /24 without RPKI or IRR authorization, while AS3758 is the legitimate origin
- ROV-enabled AS37100 discards the invalid route, and thus **has the legitimate /16 route only**
  → By seeing routing tables, AS37100 and its customers are **not aware of the potential hijacking attempt**, and tend to believe their traffic be forwarded correctly.
- However, **legacy AS6762 accepts the illegitimate route**, actually forwarding /24 traffic to AS17894

**BGP hijacking still succeeds, and becomes less spotted (stealthier), due to the incomplete ROV deployment in the current Internet?**

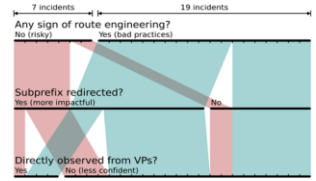
## **Approach:** empirical + simulation-based

Empirical Analysis of Stealthy Hijacking in the Wild

**Data Sources**
- RIB data from RouteViews collectors (route-views2, amsix, wide) on Oct 1, 2023 (56M routes, 86 vantage points).
- Validation: RIPE NCC RPKI, RADB IRR, WHOIS from 5 RIRs, CAIDA AS Organization dataset..

**Results**
- **26 incidents**: 19 linked to poor route engineering (e.g., outdated RPKI/IRR), 7 potential hijacks.
- **Affected:** 1,205 routes, 40 prefixes, 27 origins.

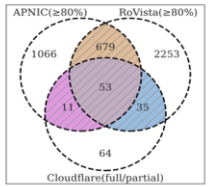
| Type | #Prefixes | #Origins | #Routes | #VPs |
|---|---|---|---|---|
| Risky incidents | 10 | 7 | 120 | 45 |
| Bad practices | 30 | 20 | 1,085 | 57 |
| Total | 40 | 27 | 1,205 | 57 |




**#0 Most wild stealthy hijacking is caused by bad route engineering practice.**

## **Evaluation:** seven takeaways

Overall Risk Level




778 ASes identified ROV-enabled by at least two sources

| Stealthy Hijacking | Sub-Prefix | Exact-Prefix |
|---|---|---|
| w/ ROV | 0.104 ▲0.104 | 0.001 ▲0.001 |
| w/o ROV | 0.000 | 0.000 |

| Direct Hijacking | Sub-Prefix | Exact-Prefix |
|---|---|---|
| w/ ROV | 0.658 ▼0.328 | 0.144 ▼0.194 |
| w/o ROV | 0.986 | 0.338 |

**#1** The overall success rate of stealthy hijacking increases from 0 to 10.4%, solely due to the partial ROV deployment in today's Internet.

## **Discussion:** limitations & future work

Discussion & Future Work

**Limitations of the approach**
- Prefix-specific routing simulation?
- Accuracy-coverage trade-off of ROV cross validation?
- Complex routing policy?

**Potential practical application**
- For ISP operation: risk assessment before peering plans
- To defend attacks: targeted probing, analysis with real-world routes, ……

**Risk countermeasures**
- Keep increasing RPKI/ROV deployment (as indicated in #3)
- Co-analyzing routing data from multiple VP to identify inconsistencies
- Collaboration among ROV-enabled ASes to share threat information
- Active blackholing on detecting stealthy hijacking (like in ROV++)

# Q&A

## Thank you!

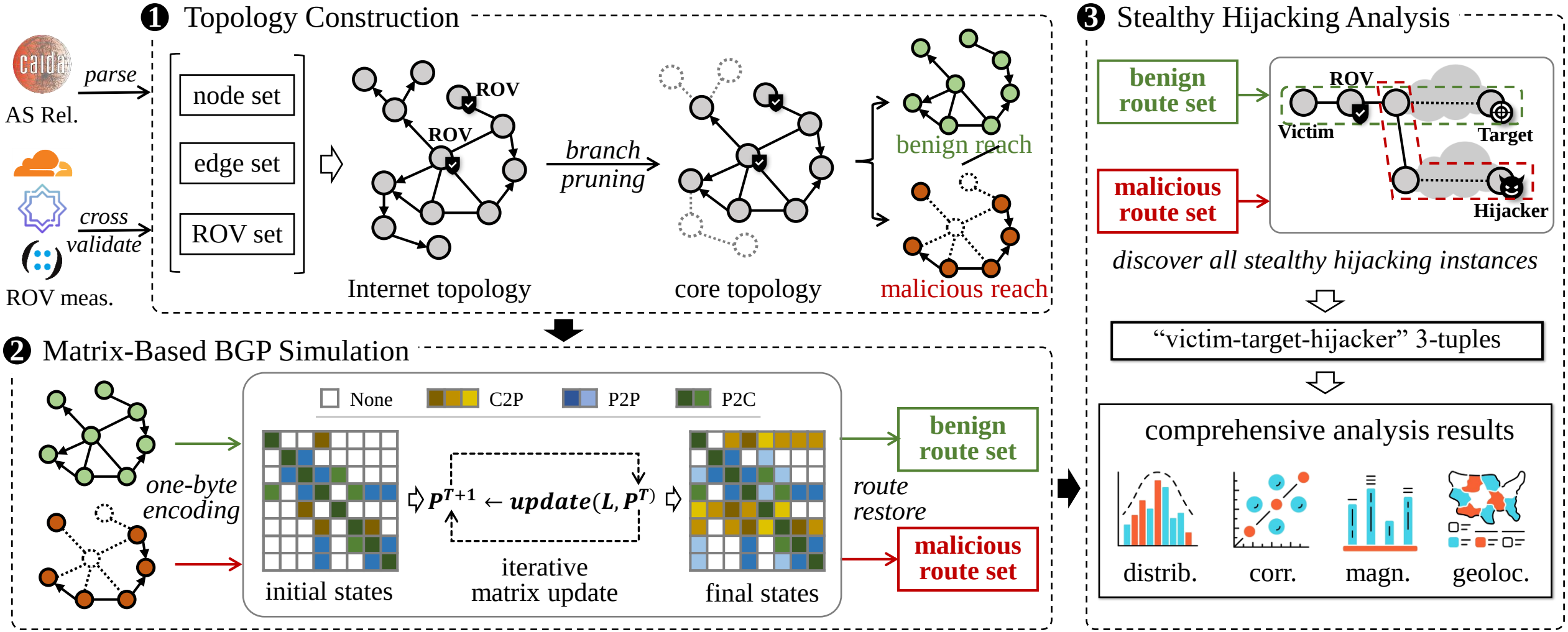
**Key Takeaways**

- Partial ROV deployment introduces stealthy hijacking risks to the current Internet.
- Risk evaluation can be achieved with complete knowledge of routes and ROV deployment.
- Our approach cross-validates multiple sources of ROV measurements and infers BGP routes.
- A 10.4% success rate of stealthy hijacking is introduced by the current ROV deployment.

**Contact:** yh-chen21@mails.tsinghua.edu.cn (Yihao Chen)

**Online Service:** https://yhchen.cn/stealthy-bgp-hijacking/

# Appendix: Simulation-Based Analysis Workflow



# Appendix: Gap in Risk Evaluation

- ROV++ [Morillo et al, NDSS'21]
  - Assume **unrealistic ROV deployment** for experiments.
  - Evaluate with **limited stealthy hijacking samples**.
  - Present **overall hijacking rate** only.

**Questions unanswered:**
The prevalence, extent, distribution, influencing factors, etc. of the risk within our real-world Internet.

Is it possible to **comprehensively** evaluate the stealthy hijacking risk introduced by the **current** ROV deployment?

**Challenges: Criteria to identify risk? Knowledge of routes? Measurement of ROV deployment? ……**