BGP Hijackers That Evade Public Route Collectors*

Presentation by
Alexandros Milolidakis
miloli@kth.se

** Based on our recent IEEE Access Journal (Link)*

Outline

- Background
- The Problem
- Lessons Learned
- Real-world Findings
- Suggestions

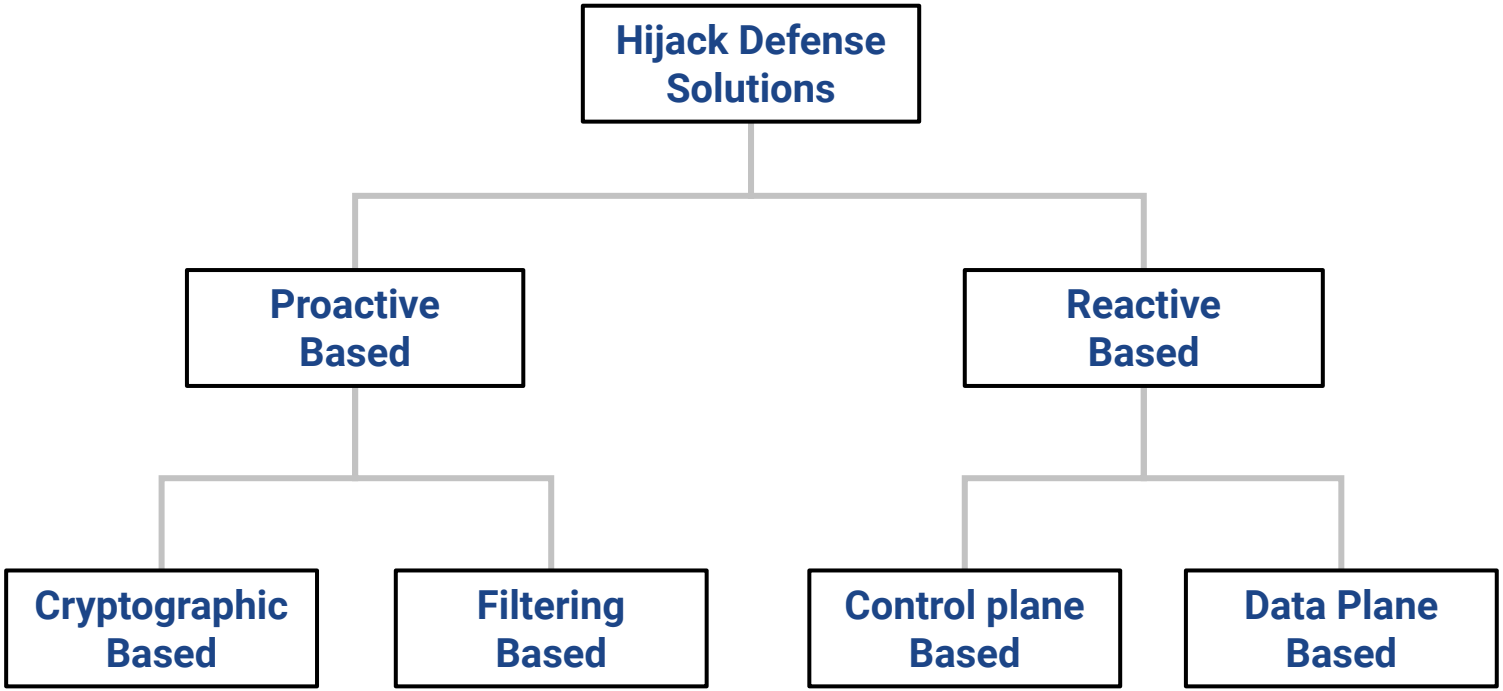
BGP Prefix Hijacking

Documented Suspicious BGP Hijacks:

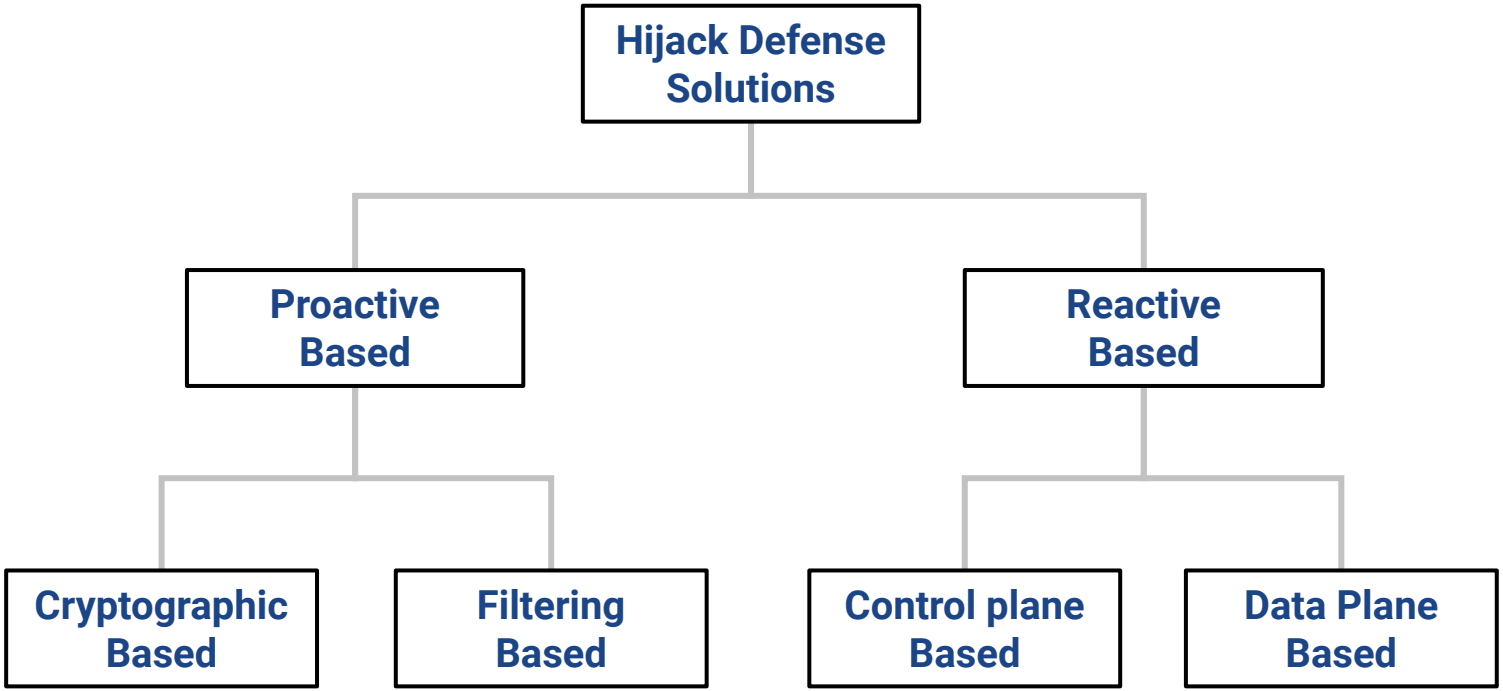
- Targets 2022: Governmental infrastructure **[1],** Cryptocurrency services **[2],** etc.
- Incidents 2021: 775 suspicious BGP hijacks **[3]**.
- Incidents 2020: 2255 suspicious BGP hijacks **[4]**.
- Incidents 2019: 1727 suspicious BGP hijacks **[4]**.

[1] *Luconi V. Et al."Impact of the first months of war on routing and latency in Ukraine", Computer Networks Journal*
[2] *https://www.kentik.com/blog/bgp-hijacks-targeting-cryptocurrency-services/*
[3] *https://www.manrs.org/2022/02/bgp-security-in-2021/*
[4] *https://www.manrs.org/2021/03/a-regional-look-into-bgp-incidents-in-2020/*

Current Solutions

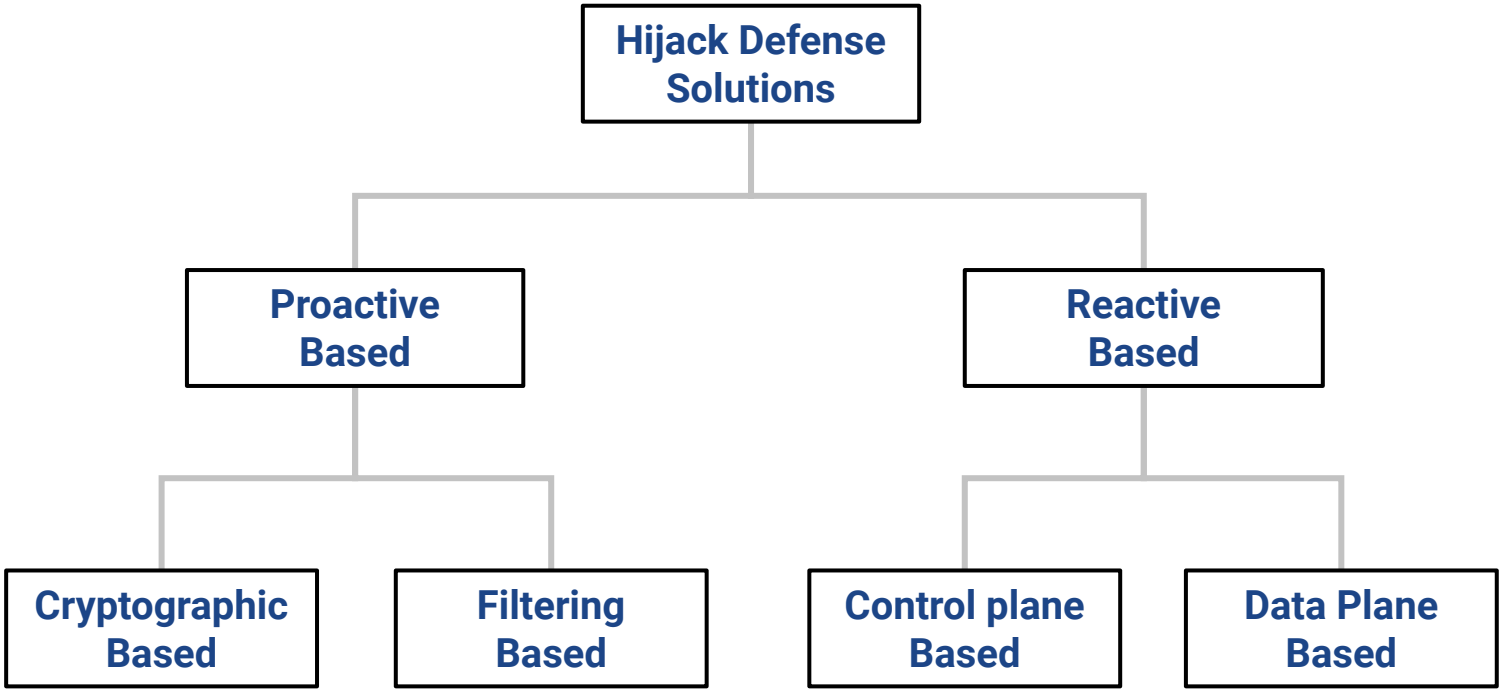


Current Solutions



Not Sufficient for all forms of hijacks (currently)

Current Solutions



Current Hijack Solutions

★ Most of current Commercial solutions rely on *Route collectors* & *Looking Glasses*.

Route Collectors (RC):

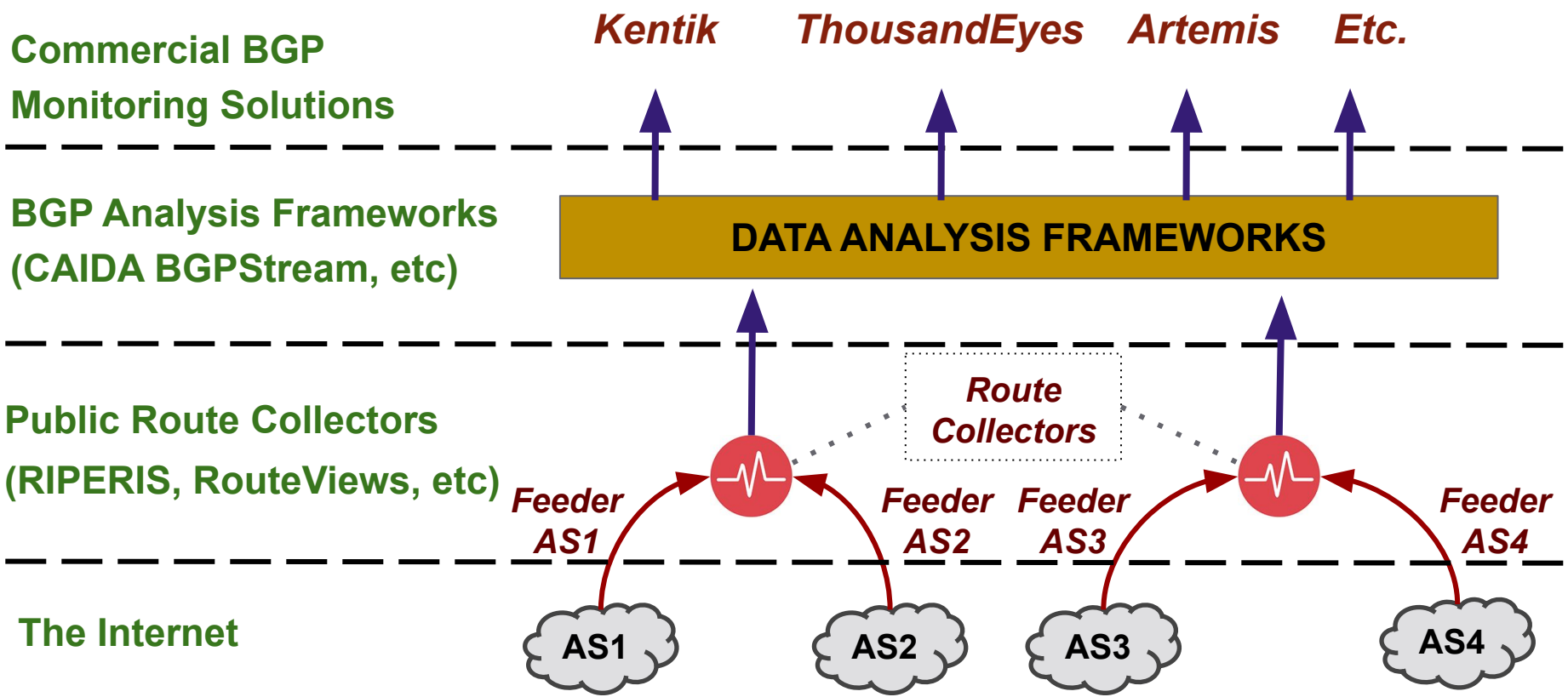
❖ BGP speaking devices that collect & report routes received from their neighbors.

Public Route Collector Infrastructure:

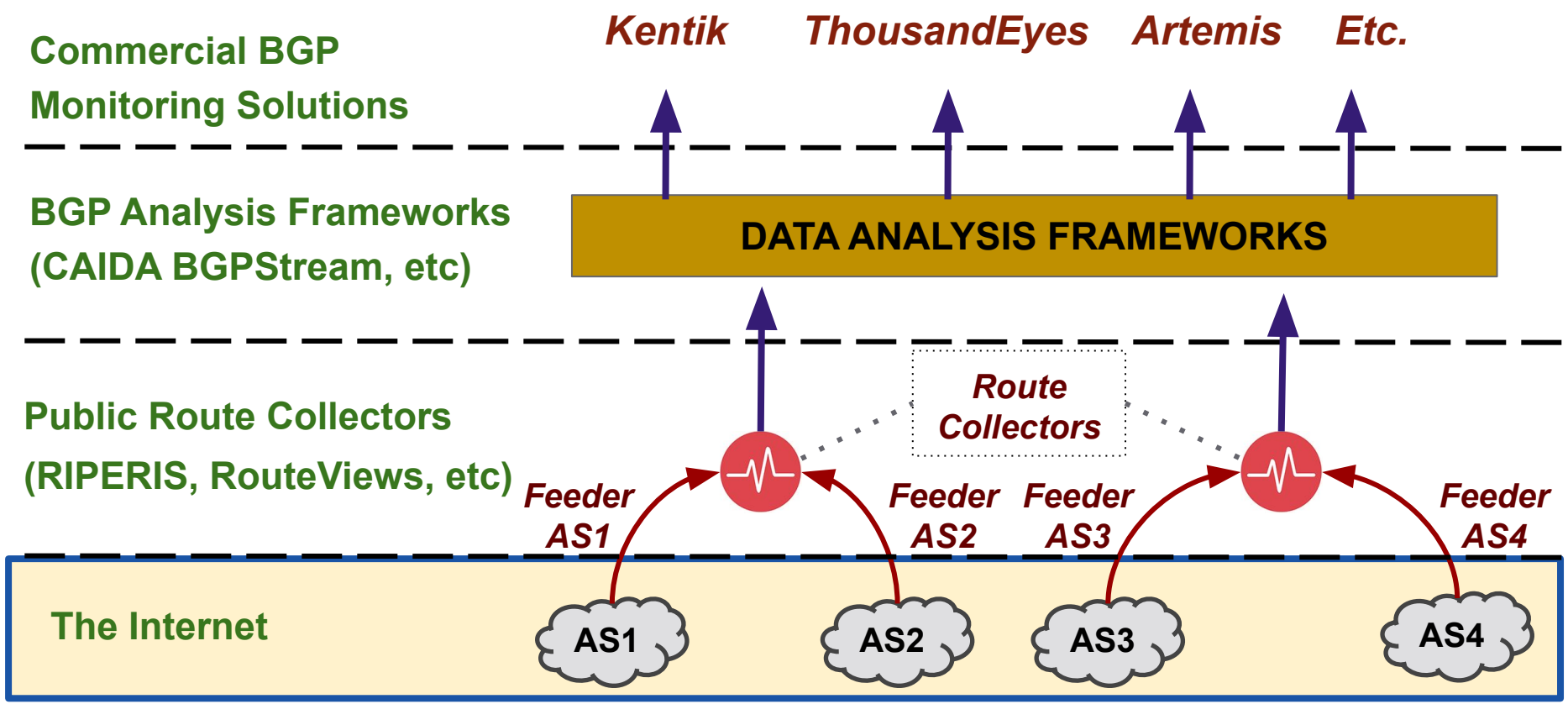
❖ Namely: RIPE-RIS, Routeviews, etc.

❖ Collection of multiple route collectors distributed around the world.

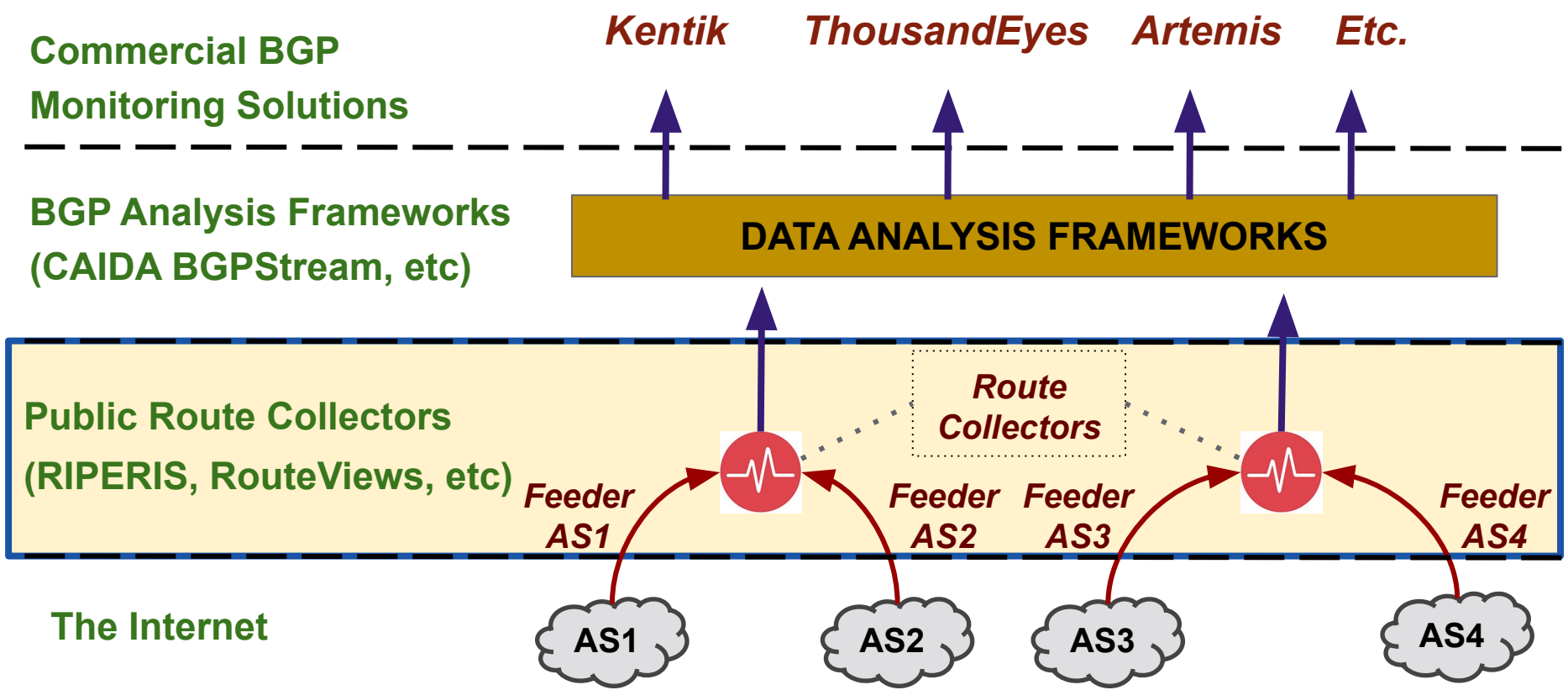
Pipeline: Route Collection by Commercial Solutions



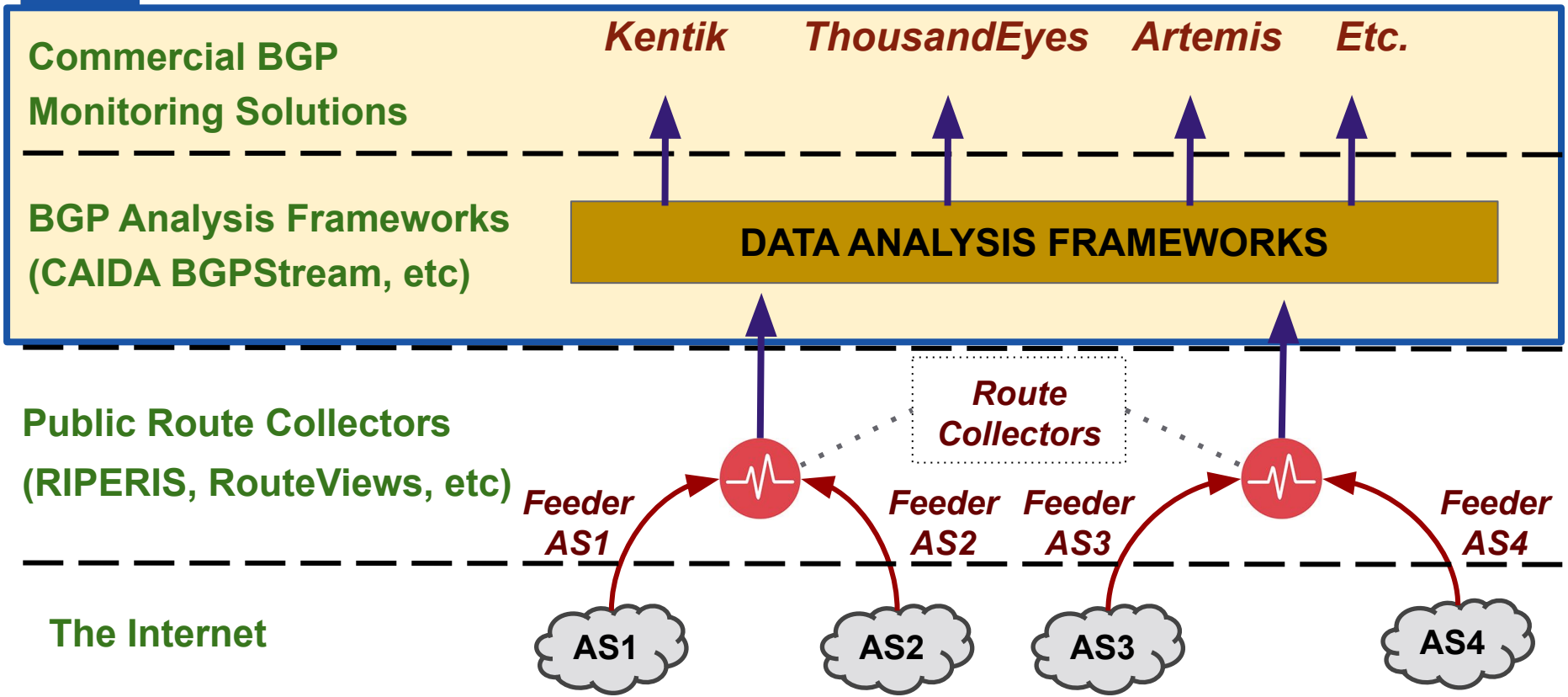
Pipeline: Route Collection by Commercial Solutions



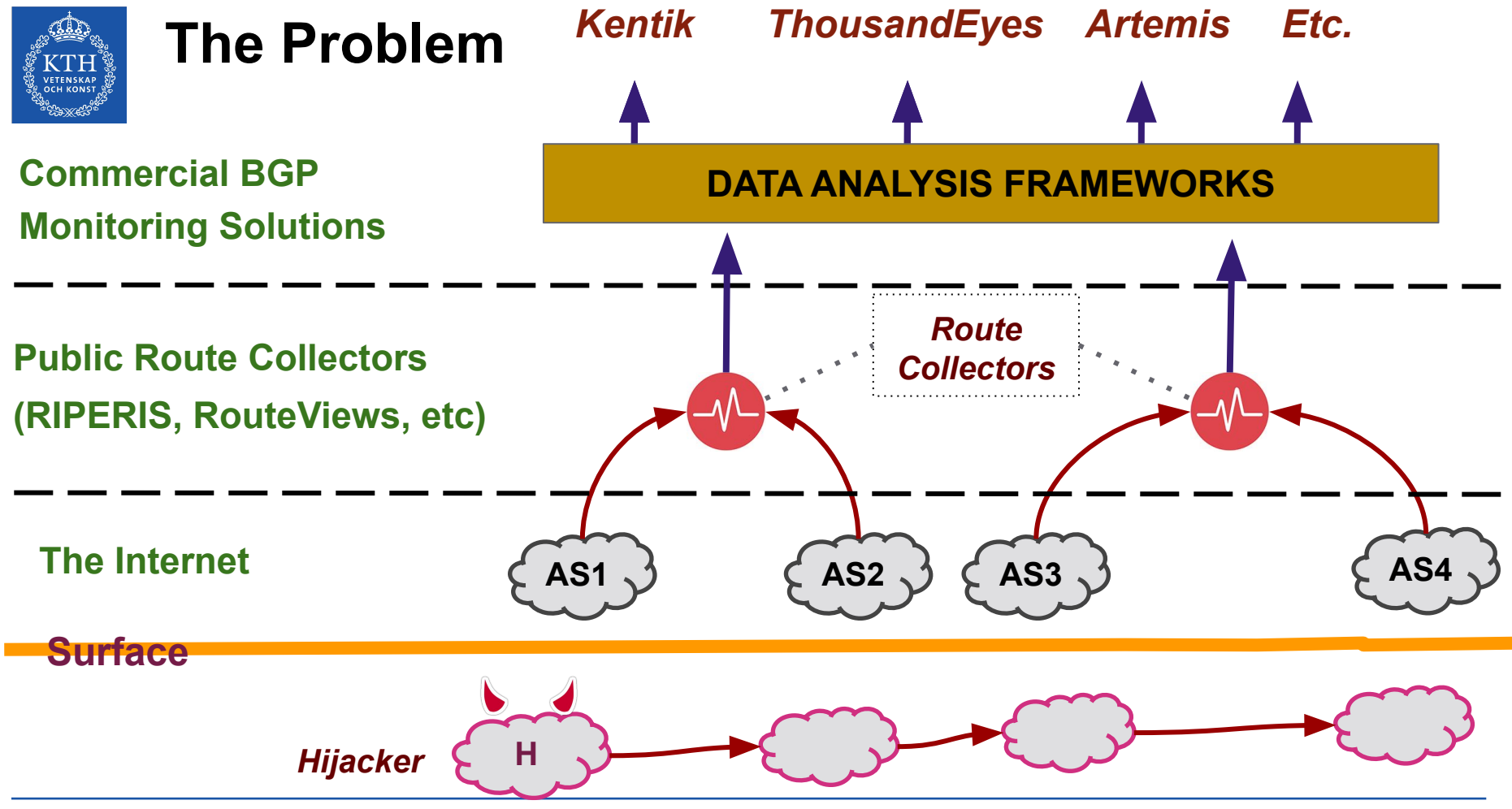
Pipeline: Route Collection by Commercial Solutions



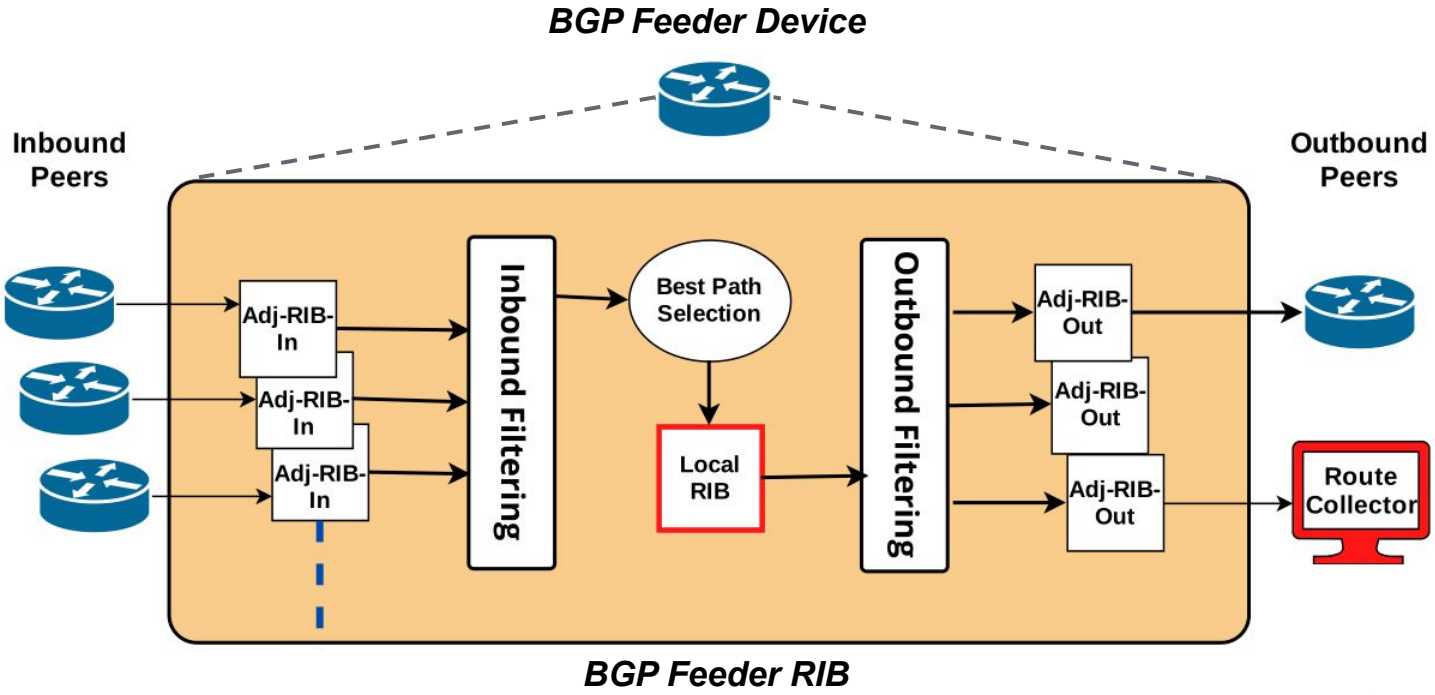
Pipeline: Route Collection by Commercial Solutions



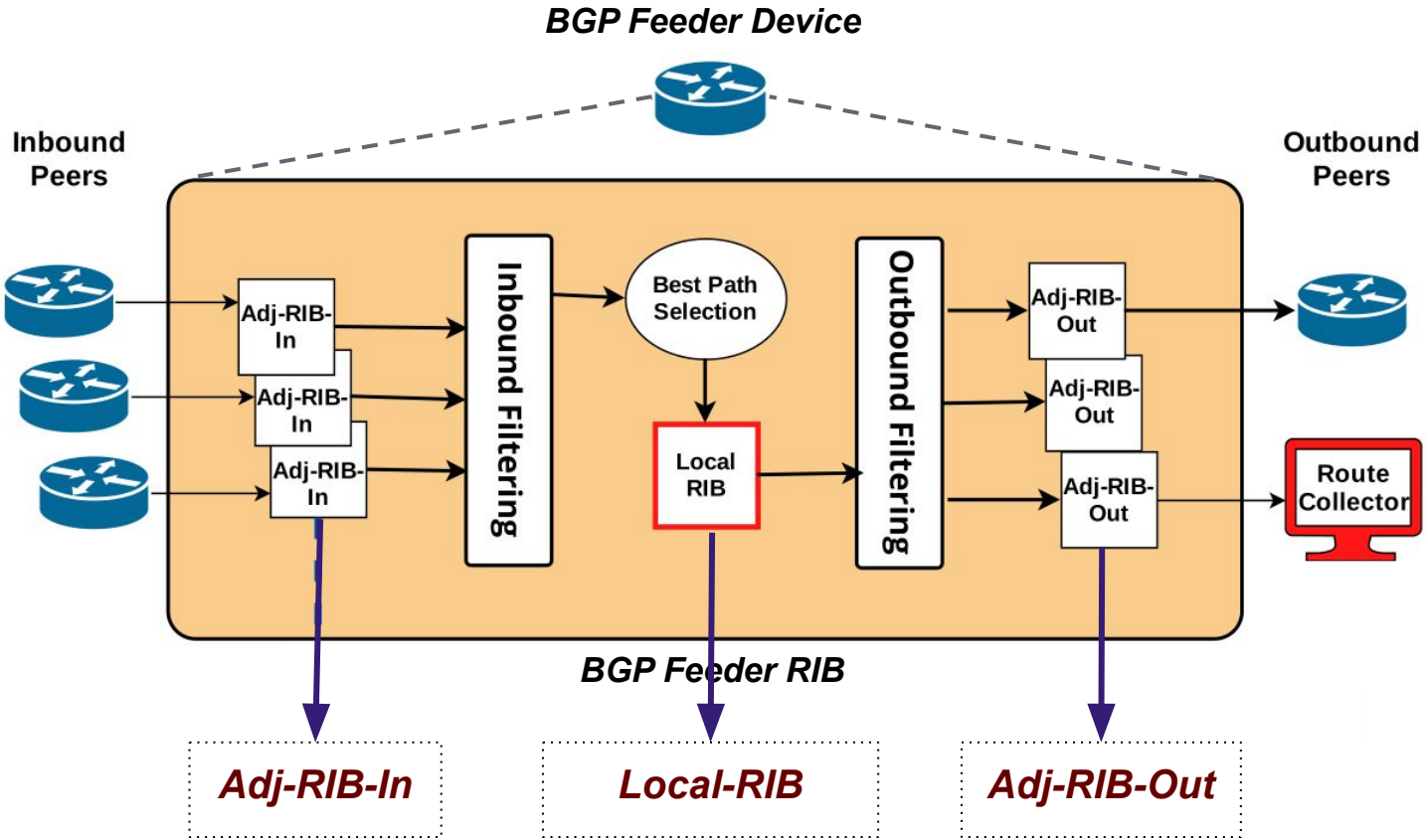
The Problem


Kentik
ThousandEyes
Artemis
Etc.
DATA ANALYSIS FRAMEWORKS
Commercial BGP
Monitoring Solutions
Public Route Collectors
(RIPERIS, RouteViews, etc)
Route
Collectors
The Internet
AS1
AS2
AS3
AS4
Surface
Hijacker
H

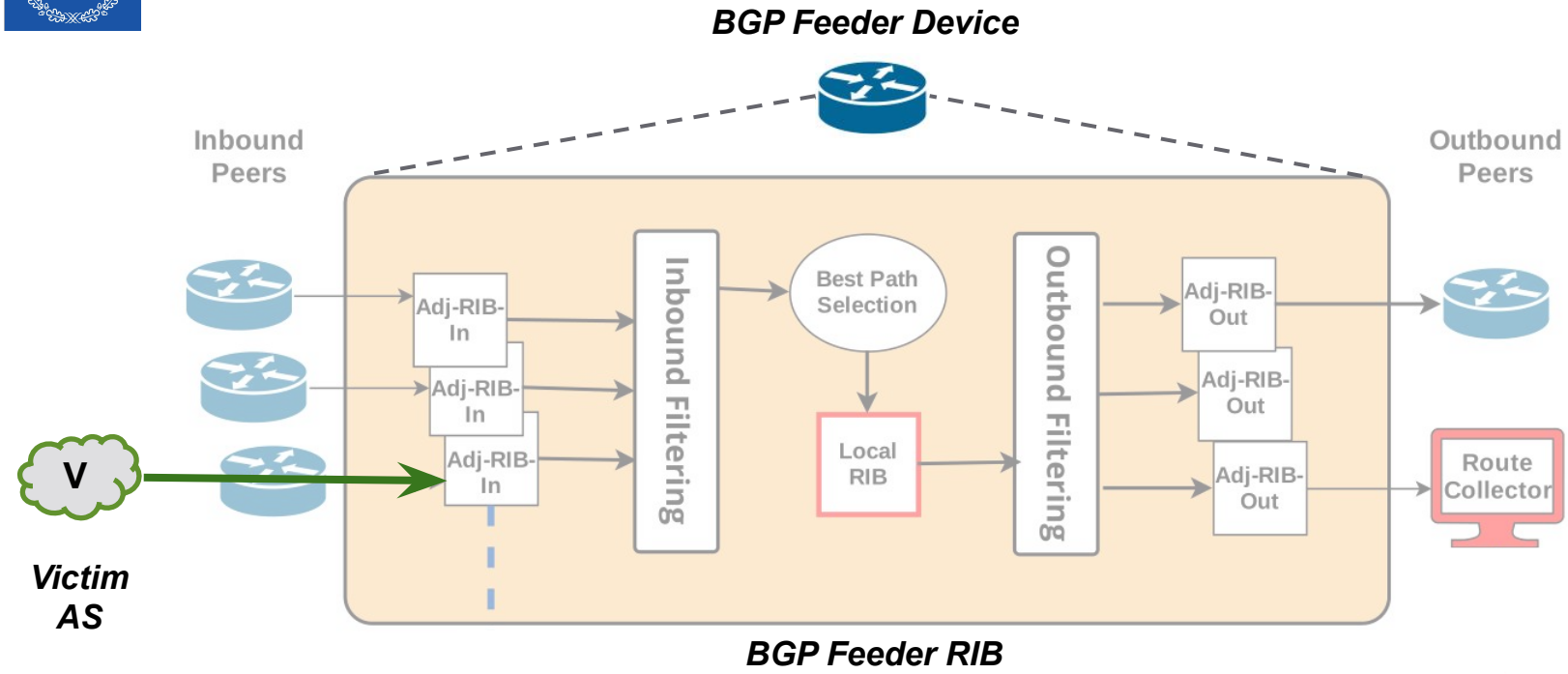
The Problem: Example of Stealthy Hijack to RC



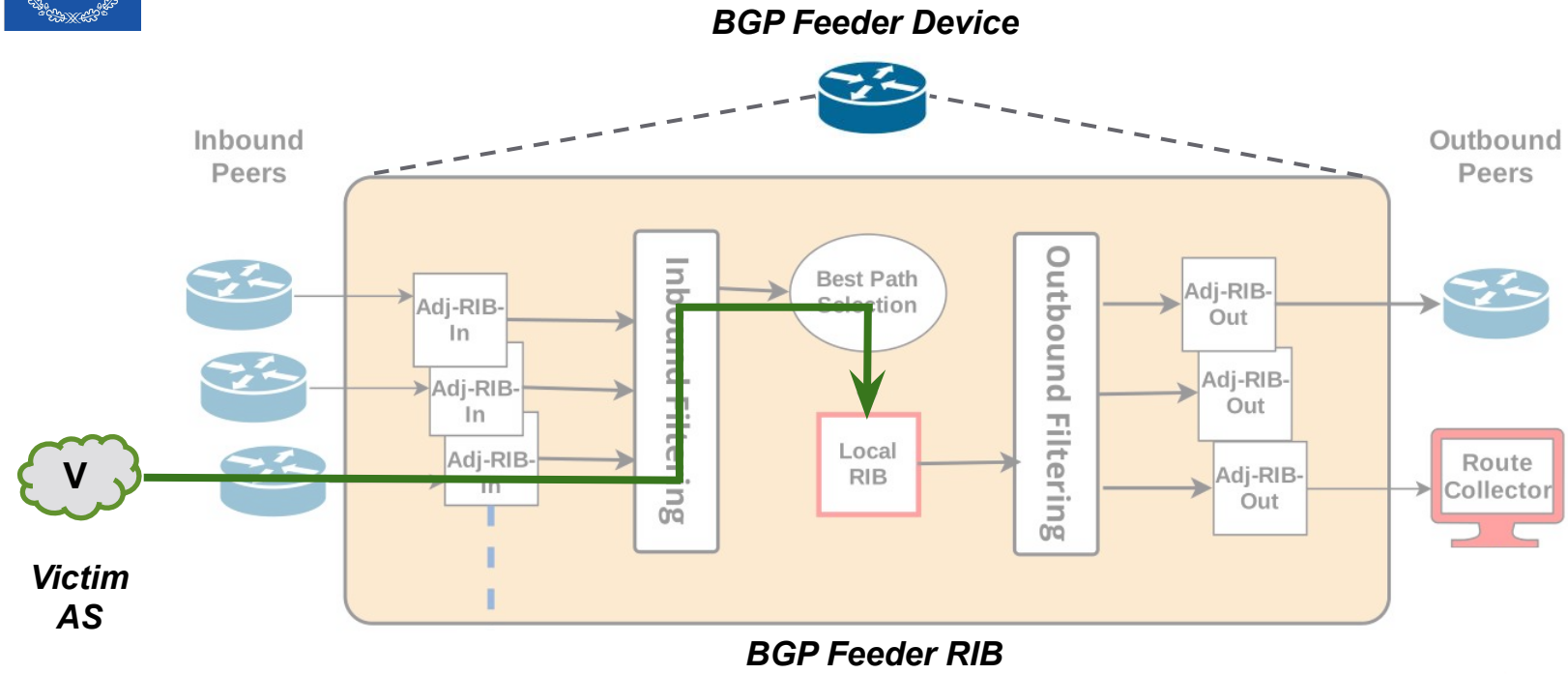
The Problem: Example of Stealthy Hijack to RC



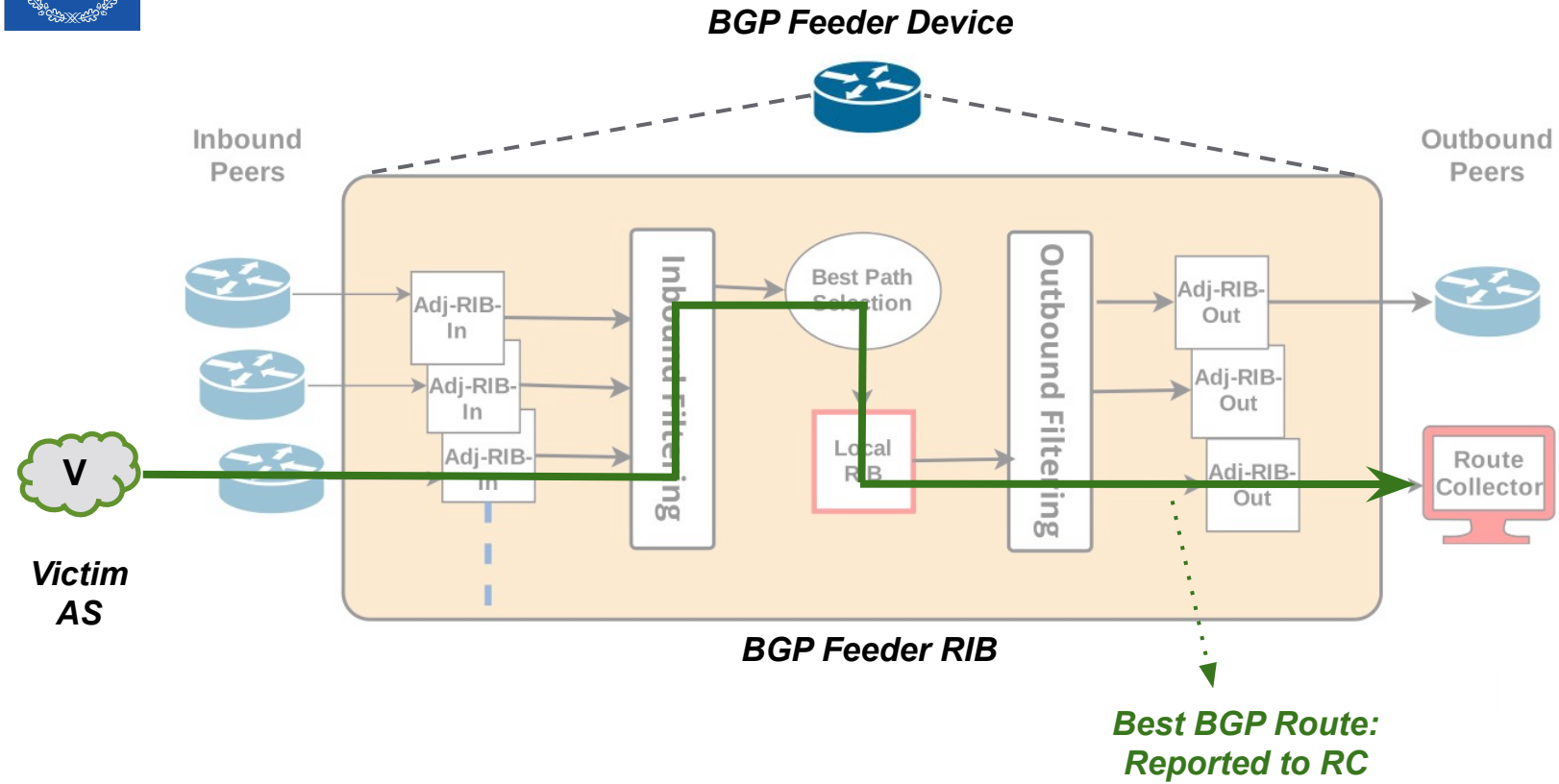
The Problem: Example of Stealthy Hijack to RC



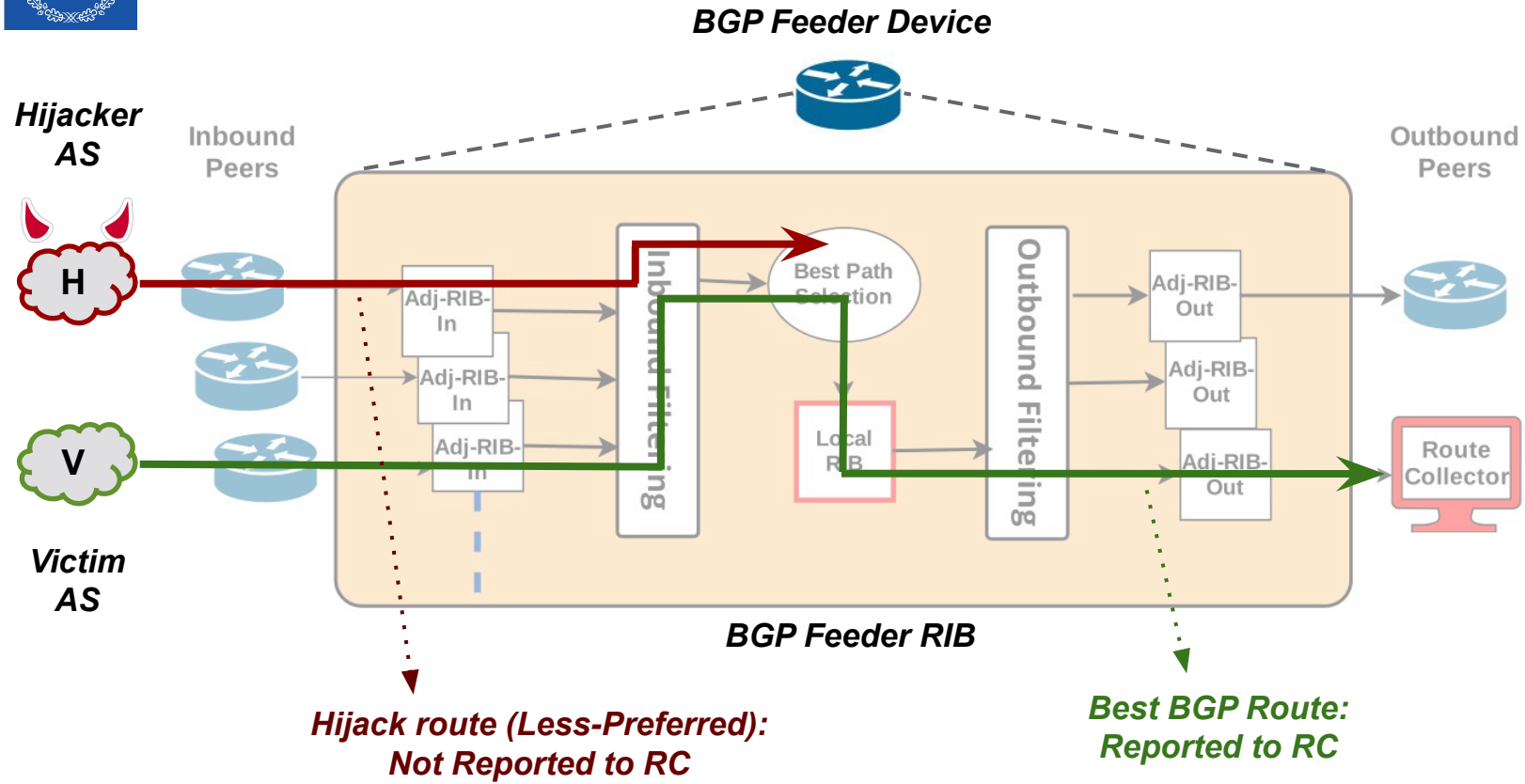
The Problem: Example of Stealthy Hijack to RC



The Problem: Example of Stealthy Hijack to RC



The Problem: Example of Stealthy Hijack to RC

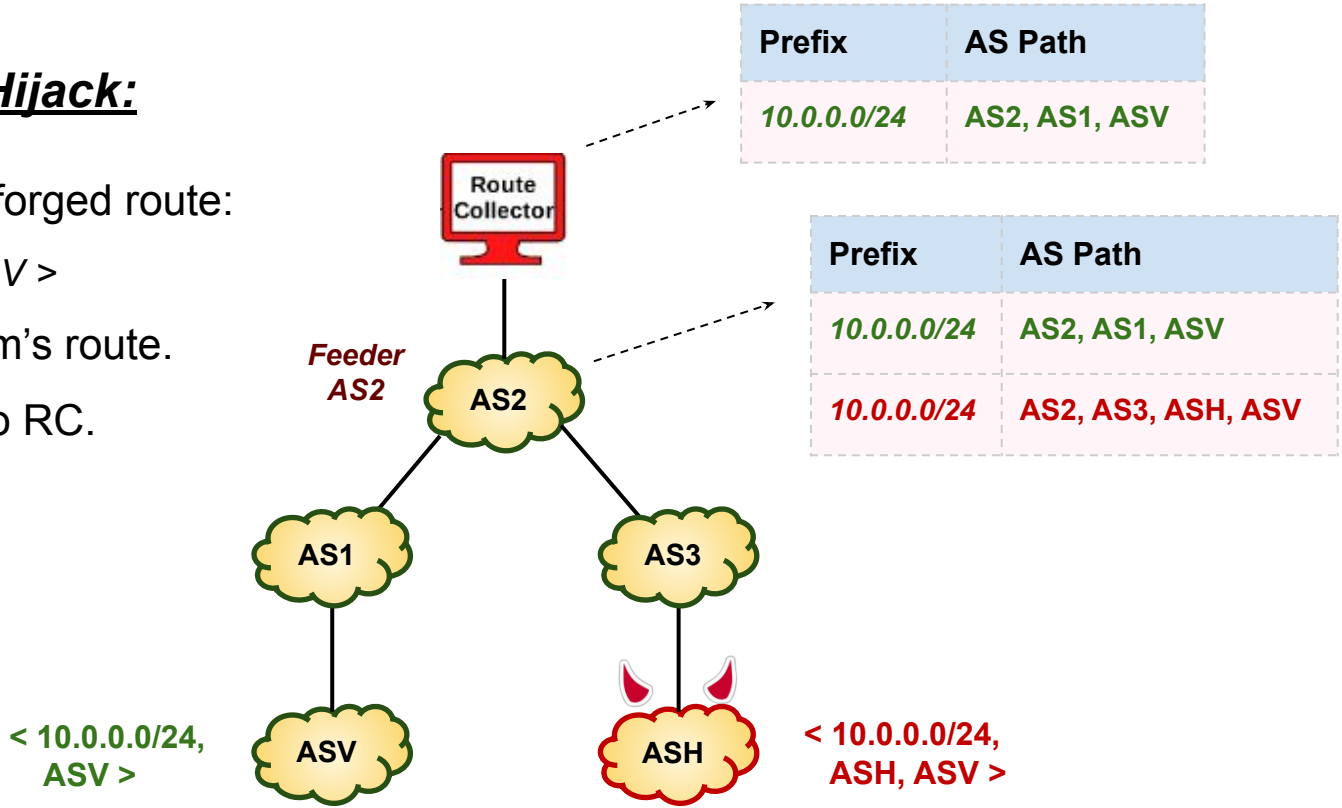


The Problem: Example of Stealthy Hijack to RC

Example of Stealthy Hijack:

- Hijacker announces forged route:

  < 10.0.0.0/24, ASH, ASV >
- AS2 prefers the victim's route.
- Hijack not reported to RC.



Presentation Topic

This Presentation:

- How capable are hijackers to design stealthy hijacks not visible by RCs?

Presentation Topic

This Presentation:

- How capable are hijackers to design stealthy hijacks not visible by RCs?

Our Experiments:

- BGP hijack Simulations.*
- Real-world experiments using the PEERING Testbed.*

* For our full experiment results: See our *journal*.

What we Learned

For a Hijacker to hide from Public RCs:

- Knowledge about which BGP feeders will report the attack matters.
- Knowledge about routing policies of other ASes matters.
- Where the hijack is exported matters.

What we Learned (1/3)

- Knowledge about feeders matters.

➔ Unaffected region feeders: Do **not** observe the hijack.

➔ Affected region feeders: Will observe the hijack.

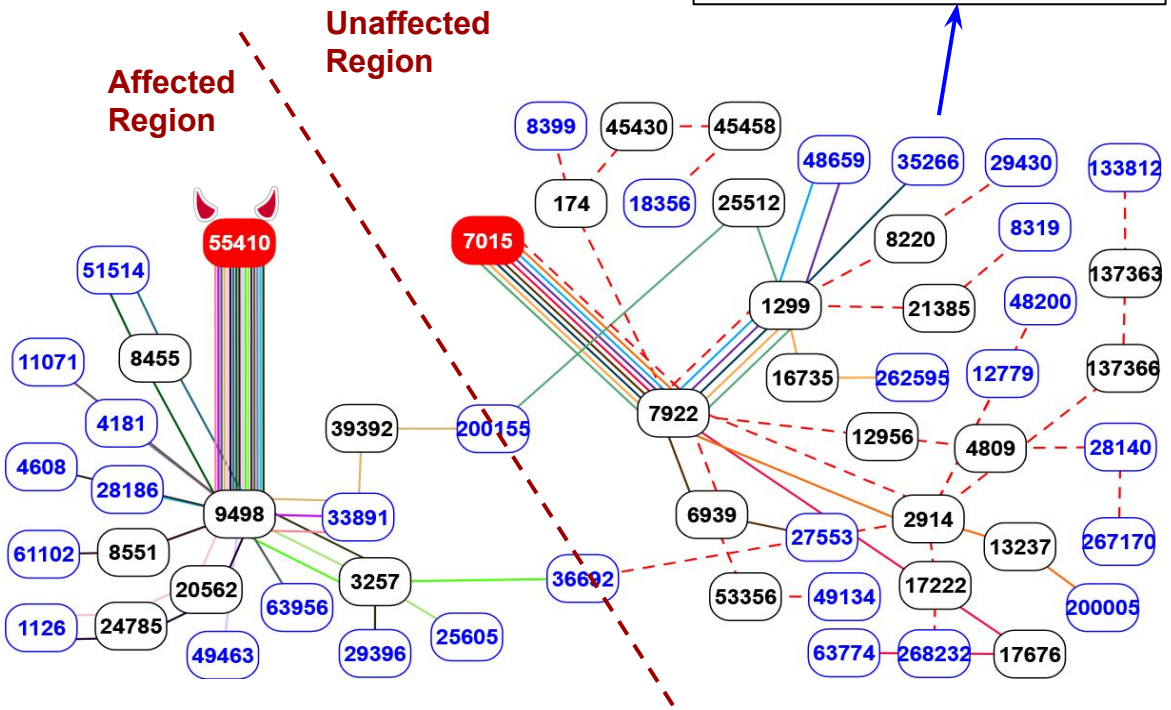


Fig: Vodafone (AS55410) leaking Comcast (AS7015) prefixes (16-04-21)
(Source: Cisco BGPstream monitoring service - visualized using BGPlay)

What we Learned (2/3)

To design not observable hijacks by public RCs:

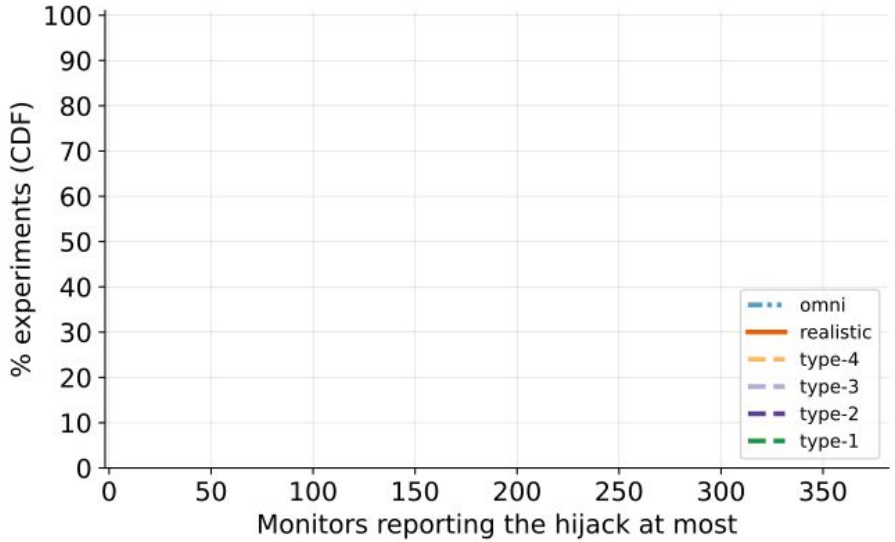
- Knowledge about which BGP feeders will report the attack matters.
- Knowledge about routing policies of other ASes matters.

What we Learned (2/3)

To design not observable hijacks by public RCs:

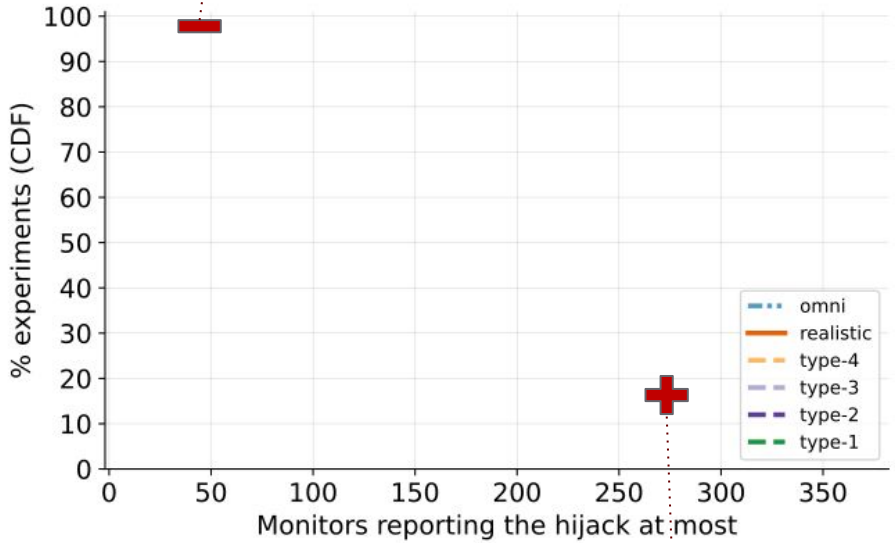
- Knowledge about which BGP feeders will report the attack matters.
- Knowledge about routing policies of other ASes matters.
  - *Baseline hijacker:* Traditional hijacker – does not deliberately avoid RCs.
  - *Realistic hijacker:* Limited knowledge inferred from routes public RCs disclose.
  - *Omniscient hijacker:* Knows routing policies of every AS in the topology.

Knowledge Routing Policies Matters – Visibility



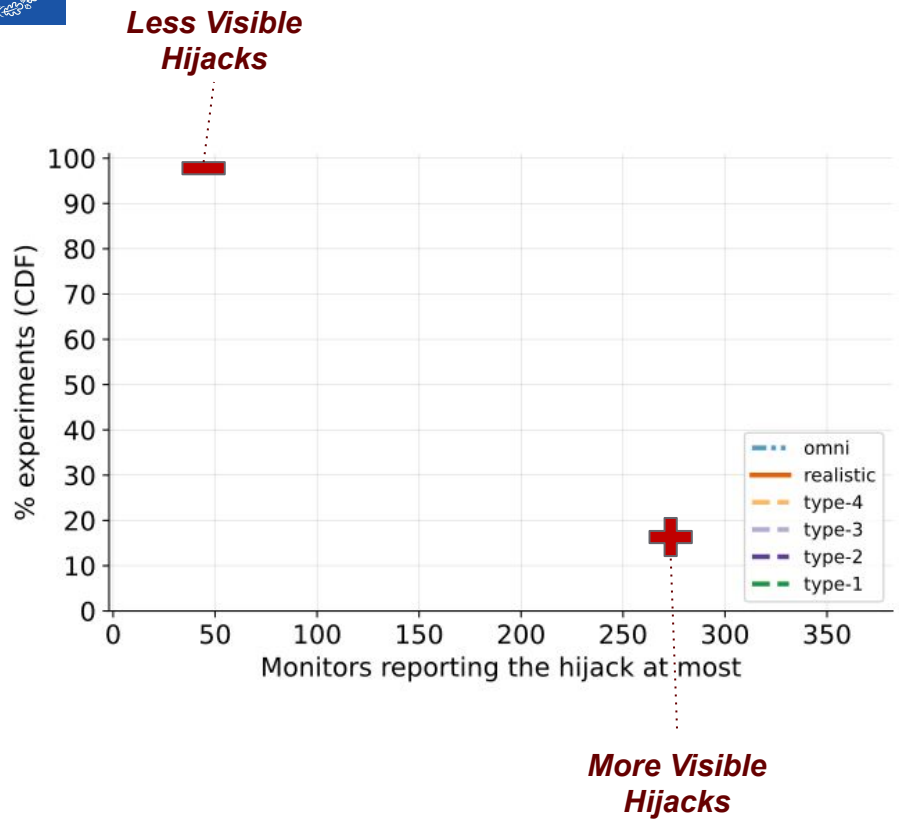
Knowledge Routing Policies Matters – Visibility

Less Visible Hijacks



More Visible Hijacks

Knowledge Routing Policies Matters – Visibility



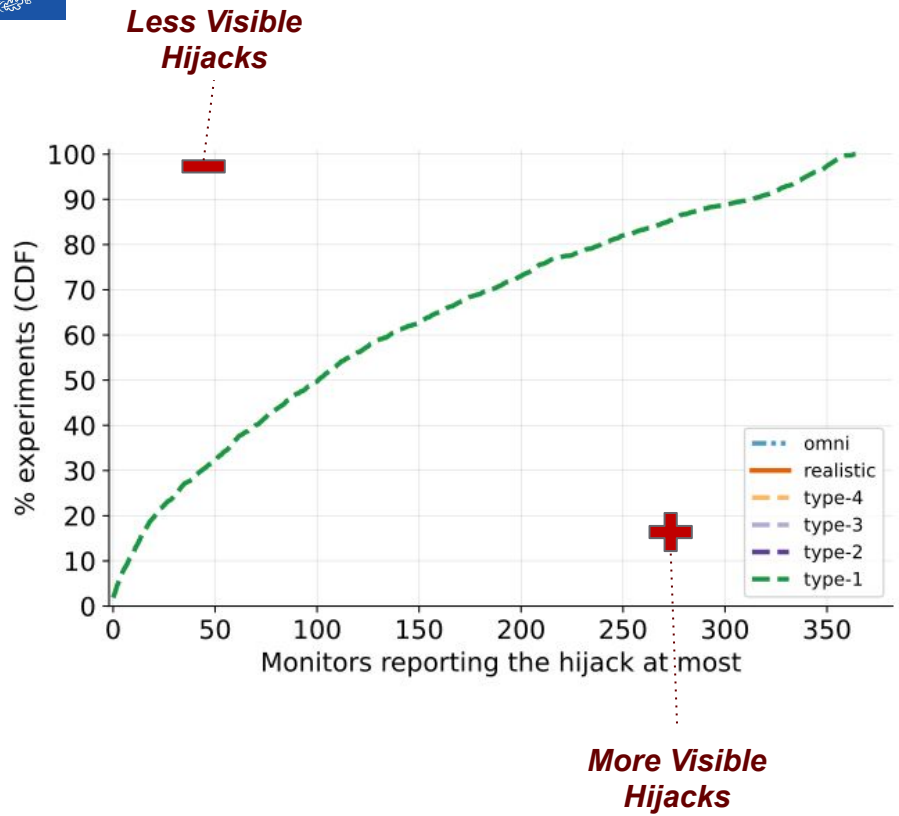
***Baseline Hijackers (shape forged paths)*:**

- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

Higher Type: *Longer* forged paths

** Visibility results based on the AS-level graph*

Knowledge Routing Policies Matters – Visibility



***Baseline Hijackers (shape forged paths)*:**

- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

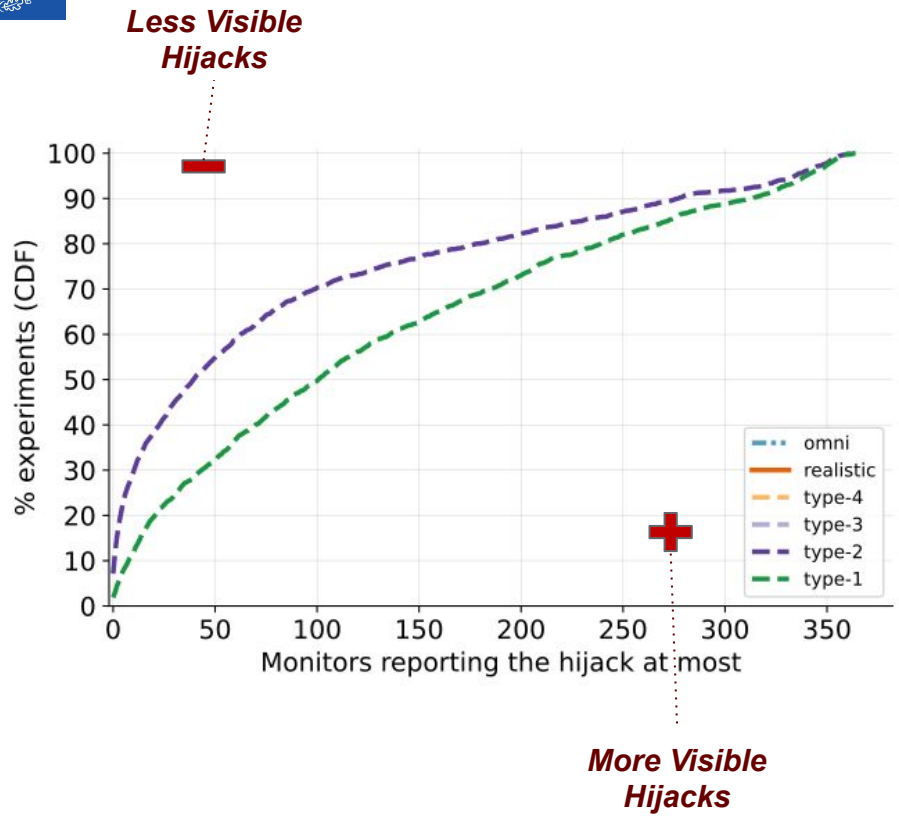
Higher Type: *Longer* forged paths

***Visibility (2K simulations)**:**

- **Type-1: 2% completely stealthy.**
- **Type-2: 7% completely stealthy.**
- **Type-3: 15% completely stealthy.**
- **Type-4: 21% completely stealthy.**

** Visibility results based on the AS-level graph*

Knowledge Routing Policies Matters – Visibility



***Baseline Hijackers (shape forged paths)*:**

- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

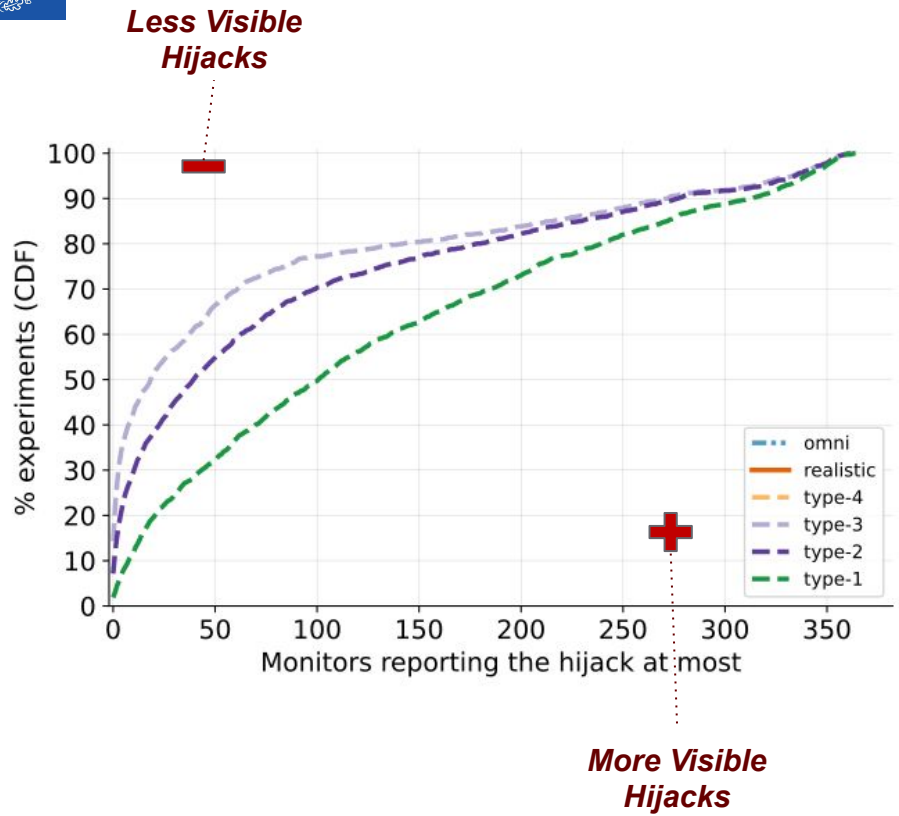
Higher Type: *Longer* forged paths

***Visibility (2K simulations)**:**

- **Type-1: 2% completely stealthy.**
- **Type-2: 7% completely stealthy.**
- **Type-3: 15% completely stealthy.**
- **Type-4: 21% completely stealthy.**

** Visibility results based on the AS-level graph*

Knowledge Routing Policies Matters – Visibility



***Baseline Hijackers (shape forged paths)*:**

- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

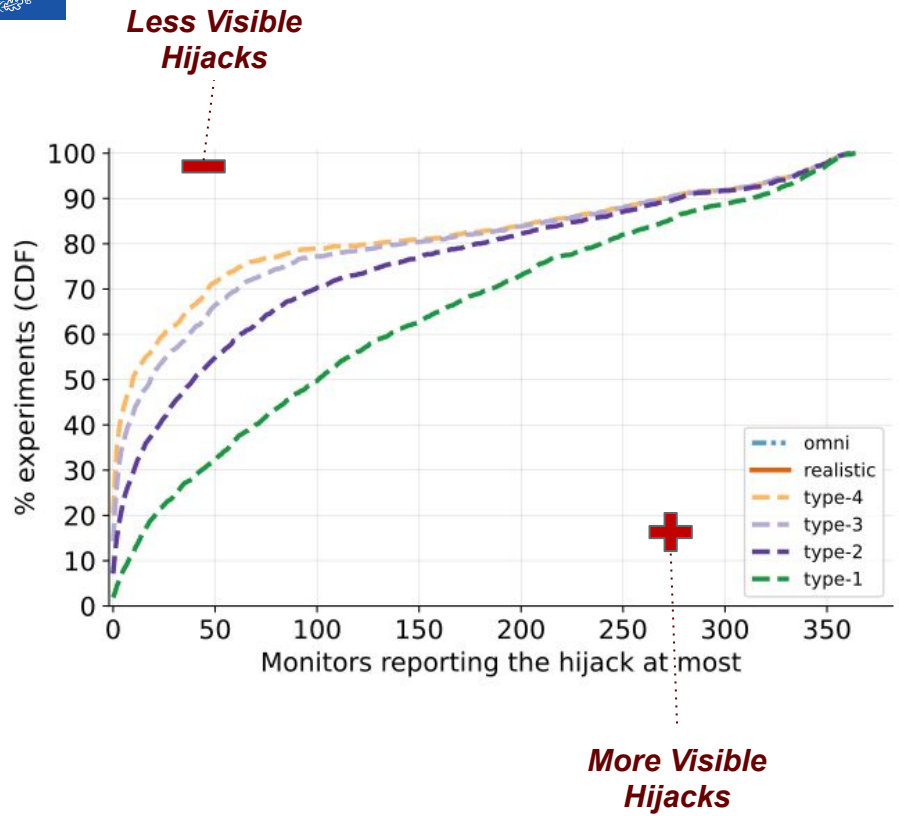
Higher Type: *Longer* forged paths

***Visibility (2K simulations)**:**

- **Type-1: 2% completely stealthy.**
- **Type-2: 7% completely stealthy.**
- **Type-3: 15% completely stealthy.**
- **Type-4: 21% completely stealthy.**

** Visibility results based on the AS-level graph*

Knowledge Routing Policies Matters – Visibility



***Baseline Hijackers (shape forged paths)*:**

- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

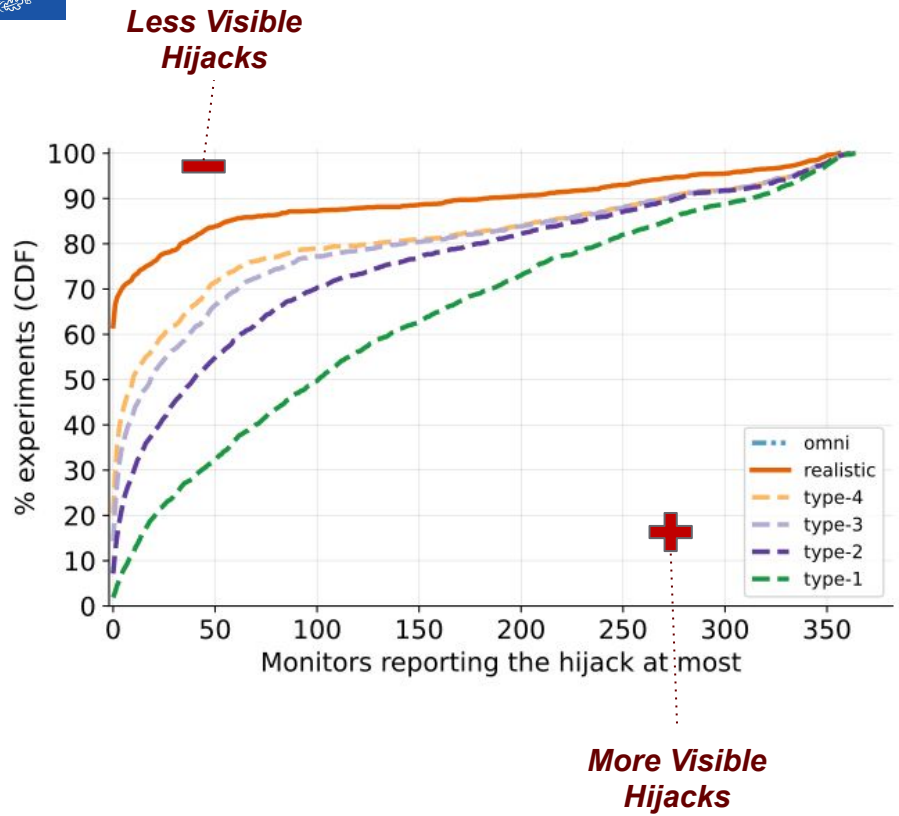
Higher Type: *Longer* forged paths

***Visibility (2K simulations)**:**

- **Type-1: 2% completely stealthy.**
- **Type-2: 7% completely stealthy.**
- **Type-3: 15% completely stealthy.**
- **Type-4: 21% completely stealthy.**

** Visibility results based on the AS-level graph*

Knowledge Routing Policies Matters – Visibility



***Baseline Hijackers (shape forged paths)*:**

- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

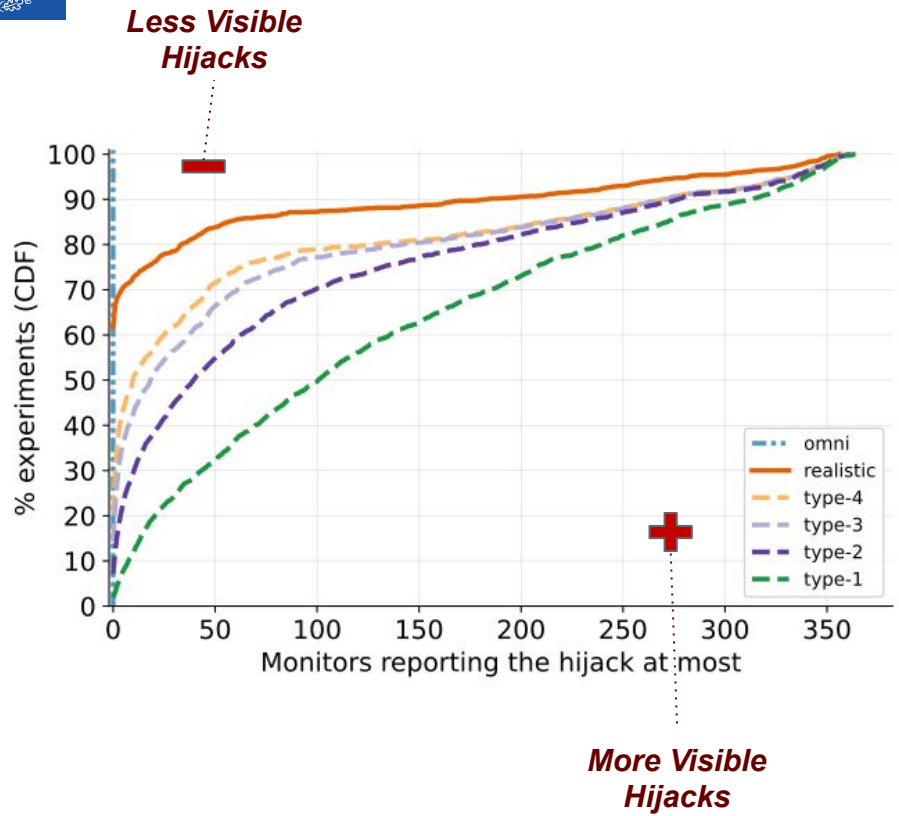
Higher Type: *Longer* forged paths

***Visibility (2K simulations)**:**

- **Type-1: 2% completely stealthy.**
- **Type-2: 7% completely stealthy.**
- **Type-3: 15% completely stealthy.**
- **Type-4: 21% completely stealthy.**
- **Real: 62% completely stealthy.**

** Visibility results based on the AS-level graph*

Knowledge Routing Policies Matters – Visibility



***Baseline Hijackers (shape forged paths)*:**

- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

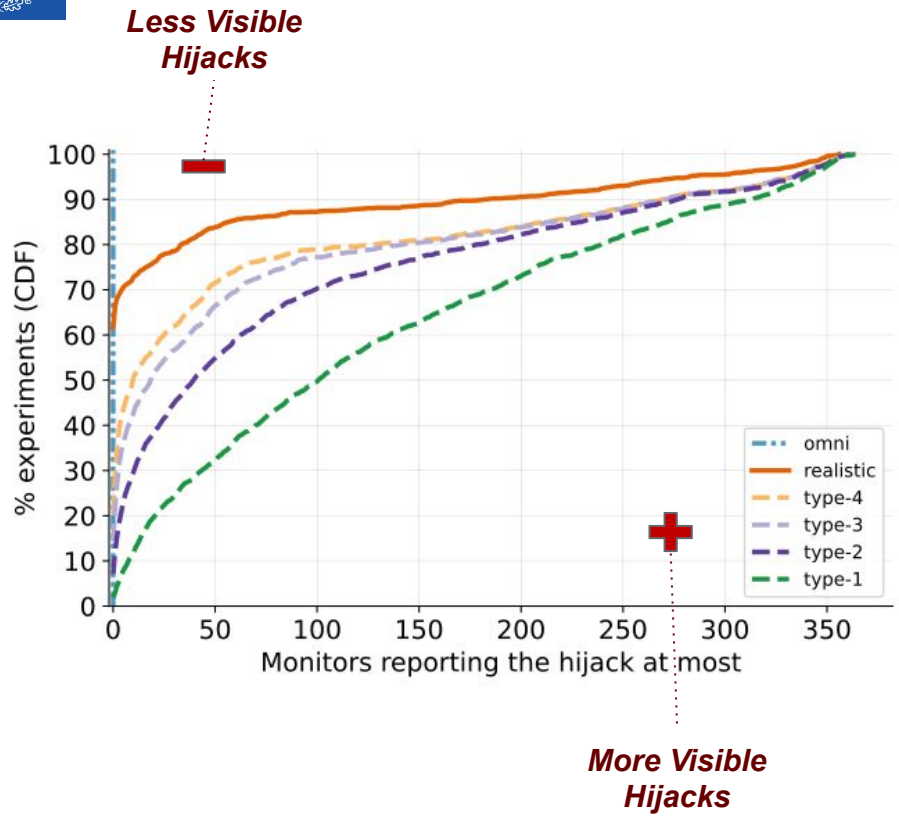
Higher Type: *Longer* forged paths

***Visibility (2K simulations)**:**

- **Type-1: 2% completely stealthy.**
- **Type-2: 7% completely stealthy.**
- **Type-3: 15% completely stealthy.**
- **Type-4: 21% completely stealthy.**
- **Real: 62% completely stealthy.**
- **Omni: 100% completely stealthy.**

** Visibility results based on the AS-level graph*

Knowledge Routing Policies Matters – Visibility



***Baseline Hijackers (shape forged paths)*:**

- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

Higher Type: *Longer* forged paths

***More Findings**:**

- **Potential Impact stealthy attacks.**
- **Future topologies: More IXP links.**
- **Future topologies: More Monitors.**

** Visibility results based on the AS-level graph*

What we Learned (3/3)

- Knowledge about which BGP feeders will report the attack matters.
- Knowledge about routing policies of other ASes matters.
- Where the hijack is exported matters.

What we Learned (3/3)

- Knowledge about which BGP feeders will report the attack matters.
- Knowledge about routing policies of other ASes matters.
- Where the hijack is exported matters.

	# Visible Simulations	*Customers*	*Peers*	*Transits*
Type-1	1963	0.3%	47%	99%
Type-4	1570	0.0%	24%	99%
Realistic	764	0.0%	3%	99%
Omni	0	0%	0%	0%

Table: % visible sims based on where the hijack is exported.

What we Learned (3/3)

- Knowledge about which BGP feeders will report the attack matters.
- Knowledge about routing policies of other ASes matters.
- Where the hijack is exported matters.

	# Visible Simulations	*Customers*	*Peers*	*Transits*
Type-1	1963	0.3%	47%	99%
Type-4	1570	0.0%	24%	99%
Realistic	764	0.0%	3%	99%
Omni	0	0%	0%	0%

Table: % visible sims based on where the hijack is exported.

Routes over Peers

- **Easier to influence:**
  Path lengths matter more for such neighbors.

Routes over Transit Providers

- **Harder to influence:**
  Business relations matter more.

What we Learned (3/3)

- Knowledge about which BGP feeders will report the attack matters.
- Knowledge about routing policies of other ASes matters.
- Where the hijack is exported matters.

	# Visible Simulations	*Customers*	*Peers*	*Transits*
Type-1	1963	0.3%	47%	99%
Type-4	1570	0.0%	24%	99%
Realistic	764	0.0%	3%	99%
Omni	0	0%	0%	0%

Table: % visible sims based on where the hijack is exported.

Realistic Hijackers

- **Hijacks easier to hide when exported to Peers.**
- **Harder to hide when exported to transits.**

Omni Hijackers

- **Completely stealthy.**

Real World Evaluation: PEERING Testbed

- Knowledge about which BGP feeders will report the attack matters.
- Knowledge about routing policies of other ASes matters.
- Where the hijack is exported matters.

Real World Evaluation: PEERING Testbed

- Knowledge about which BGP feeders will report the attack matters.
- Knowledge about routing policies of other ASes matters.
- Where the hijack is exported matters.

Real World Set-up

- ***Testbed:*** PEERING Testbed to emulate BGP hijacks.
- ***Victim:*** Testbed site at *Wisconsin*.
- ***Hijacker:*** Testbed site at *GRNET* and *AMS-IX*.

Experiment Goals

➔ ***Goal:*** Design a stealthy hijack not observable by public RCs.

➔ **(1):** Ability of hijacker to identify all dangerous monitors.

➔ **(2):** Ability of hijacker to circumvent the hijack from reaching RCs.

Binary classification of monitors

❖ ***Safe****:* Will **not** report the attack.

❖ ***Dangerous****:* Will report the attack.

Why Classifying the Monitors Matters

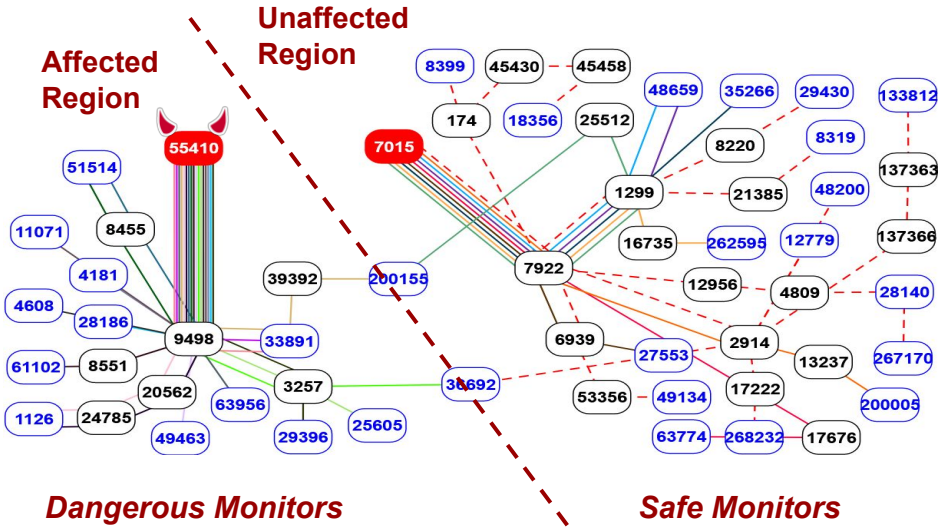
➔ ***Goal:*** Design a stealthy hijack not observable by public RCs.

➔ **(1):** Ability of hijacker to identify all dangerous monitors.

➔ **(2):** Ability of hijacker to circumvent the hijack from reaching RCs.

Binary classification of monitors

- ***Safe****:* Will **not** report the attack.
- ***Dangerous****:* Will report the attack.



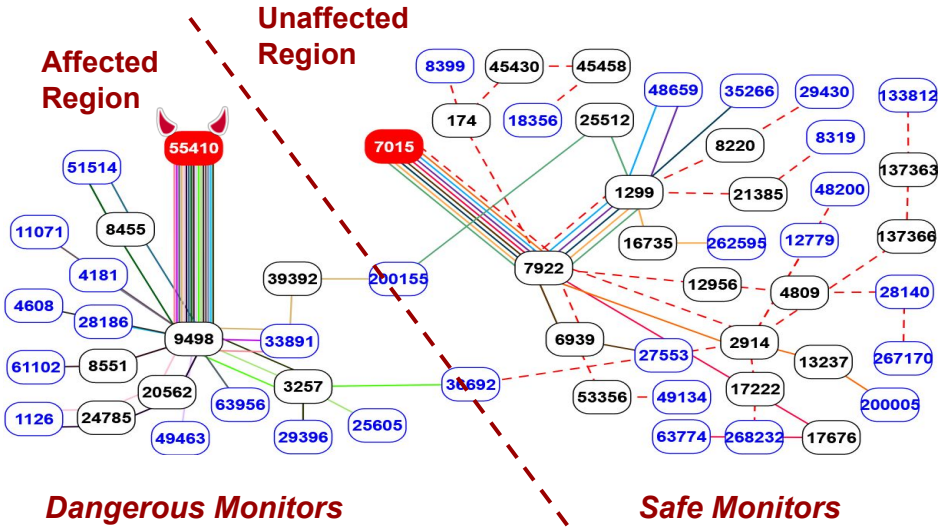
Why Classifying the Monitors Matters

- ➔ ***Goal:*** Design a stealthy hijack not observable by public RCs.
- ➔ **(1):** Ability of hijacker to identify all dangerous monitors.
- ➔ **(2):** Ability of hijacker to circumvent the hijack from reaching RCs.

Binary classification of monitors

- ❖ ***Safe****:* Will **not** report the attack.
- ❖ ***Dangerous****:* Will report the attack.

- ❖ A Proximity Classifier (AS-path lengths).
- ❖ A business relationship Classifier (Gao-Rexford).



Findings: Proximity vs Business Classifier

		GRNET Transit ASN 5408	*AMS Transit ASN 8283*	*AMS Transit ASN 12859*	*AMS Peer ASN 9002*	*AMS Peer ASN 6461*	*AMS Peer ASN 52320*
# Total Monitors							
% Monitors Correctly Classified Proximity Classifier	*Accuracy*						
	Dangerous (Safe)						
% Monitors Correctly Classified Business Classifier	*Accuracy*						
	Dangerous (Safe)						

Findings: Proximity vs Business Classifier

		GRNET Transit ASN 5408	*AMS Transit ASN 8283*	*AMS Transit ASN 12859*	*AMS Peer ASN 9002*	*AMS Peer ASN 6461*	*AMS Peer ASN 52320*
# Total Monitors		663	695	683	652	653	653
% Monitors Correctly Classified Proximity Classifier	*Accuracy*						
	Dangerous (Safe)						
% Monitors Correctly Classified Business Classifier	*Accuracy*						
	Dangerous (Safe)						

Findings: Proximity vs Business Classifier

		GRNET Transit ASN 5408	*AMS Transit ASN 8283*	*AMS Transit ASN 12859*	*AMS Peer ASN 9002*	*AMS Peer ASN 6461*	*AMS Peer ASN 52320*
# Total Monitors		663	695	683	652	653	653
% Monitors Correctly Classified Proximity Classifier	*Accuracy*	78%	74%	84%	97%	93%	99%
	Dangerous (Safe)	13% *(99%)*	62% *(93%)*	75% *(91%)*	100% *(97%)*	**10%** *(94%)*	100% *(99%)*
% Monitors Correctly Classified Business Classifier	*Accuracy*						
	Dangerous (Safe)						

Findings: Transit Providers

Proximity Classifier: Average Accuracy = 78%

NOT sufficient to identify all dangerous monitors

(Overestimates Safe Monitors)

Findings: IXP Peers

Proximity Classifier: Average Accuracy = 96%

Possible to identify all dangerous monitors

(But outliers may exist)

Findings: Proximity vs Business Classifier

		GRNET Transit ASN 5408	*AMS Transit ASN 8283*	*AMS Transit ASN 12859*	*AMS Peer ASN 9002*	*AMS Peer ASN 6461*	*AMS Peer ASN 52320*
# Total Monitors		663	695	683	652	653	653
% Monitors Correctly Classified Proximity Classifier	*Accuracy*	78%	74%	84%	97%	93%	99%
	Dangerous (Safe)	13% *(99%)*	62% *(93%)*	75% *(91%)*	100% *(97%)*	**10%** *(94%)*	100% *(99%)*
% Monitors Correctly Classified Business Classifier	*Accuracy*	90%	92%	89%	*Same*	*Same*	*Same*
	Dangerous (Safe)	95% *(89%)*	96% *(86%)*	97% *(81%)*	*Same*	*Same*	*Same*

Findings: Transit Providers

Business Classifier: Average Accuracy = 90%

Dangerous monitor misclassifications reduced by <= 91%

(At the cost of misclassifying some safe monitors)

Findings: IXP Peers

Practically Unchanged

Suggestions: Dealing with Hijackers that Avoid RCs

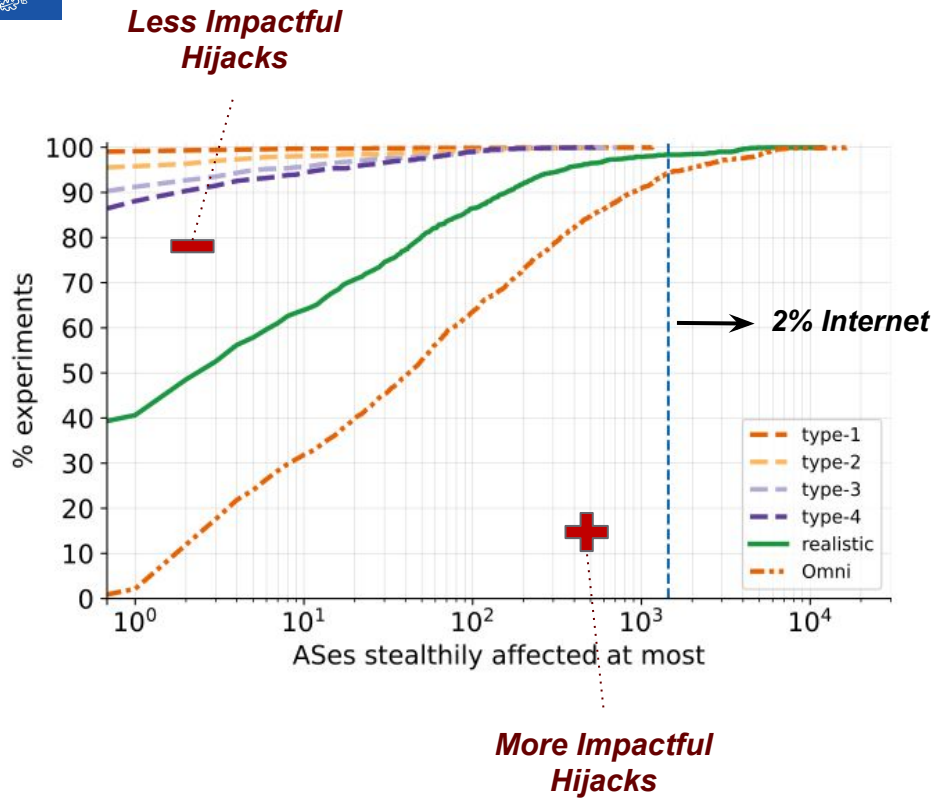
- RQ: How vulnerable are Route Collectors to stealthy attacks?
- Problem: Route collectors may be vulnerable to stealthy attacks if:
  - **(1)** BGP Feeders reports their best routes to RC and
  - **(2)** The Route Collector is public.

- Prevention methods:
  - Better BGP filtering / Following best practices (ASPA helps!).
  - New feeders: feeders in more strategic locations.
  - Smarter feeders: Forwarding suspicious routes to RC (not just the best route).
  - Feeders Forwarding all routes to RCs (BMP).

Questions?

Appendix

Knowledge Routing Policies Matters – Impact



***Baseline Hijackers (forged path shape)*:**

- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

Baseline Hijackers:

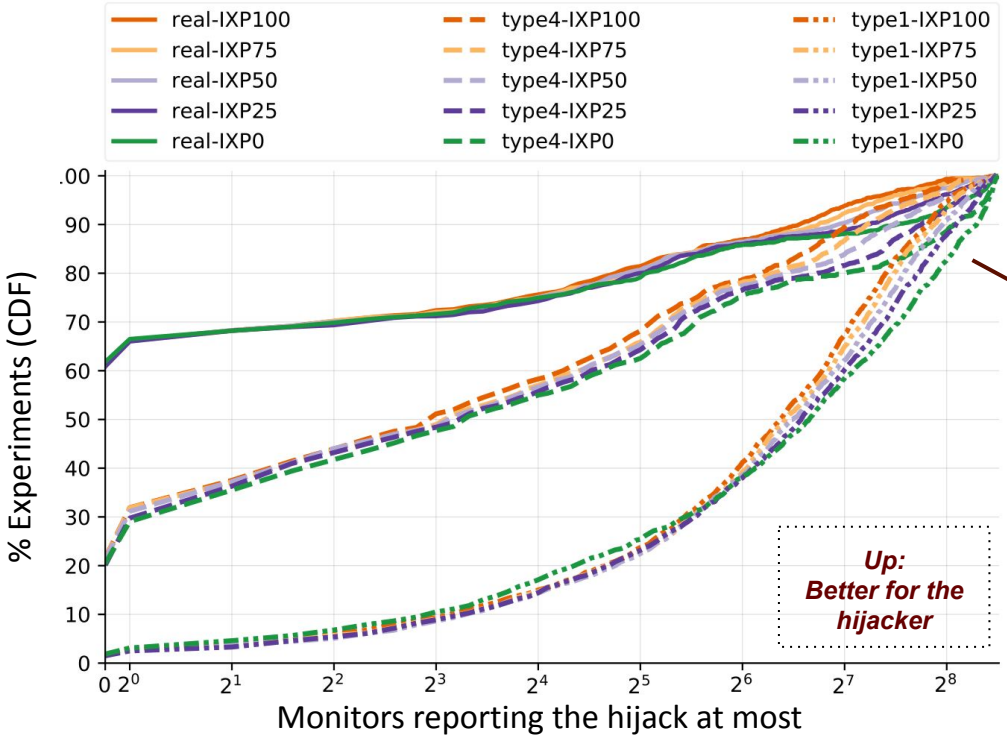
Cannot stealthily intercept > 2% Internet

Realistic & Omni Hijackers:

- **Stealthily intercepts > 2% Internet: 1.65% and 5.65% sims (respectively)**
- **Up to *16.2% & 23.5%* Internet Stealthily intercepted (respectively)**

** Results based on the AS-level graph*

Appendix – Topologies With More IXP Links



Adding more IXP links

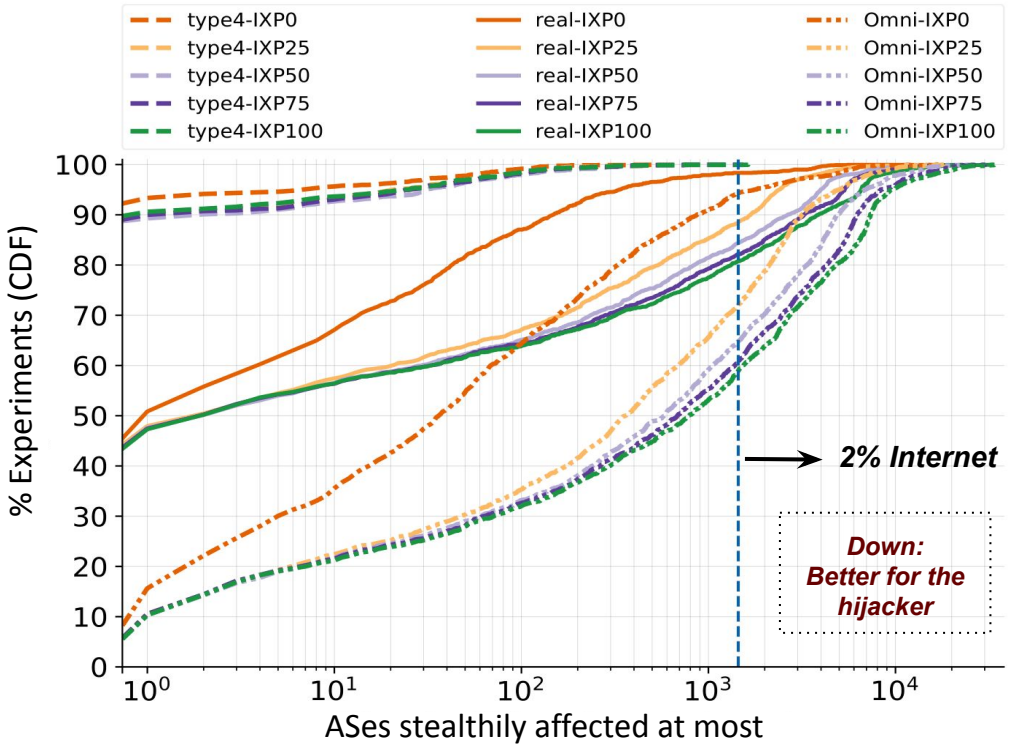
- No impact to success rate
- Visible hijacks: stealthier

90th percentile visibility

- Type-1: 28% less monitors
- Type-4: 50.9% less monitors
- Realistic: 48.3% less monitors
- Omni: Still invisible

** Results based on the AS-level graph*

Appendix – Topologies With More IXP Links



Adding more IXP links

- **Stealthy hijacks more impactful**

Traditional Topology (IXP0)

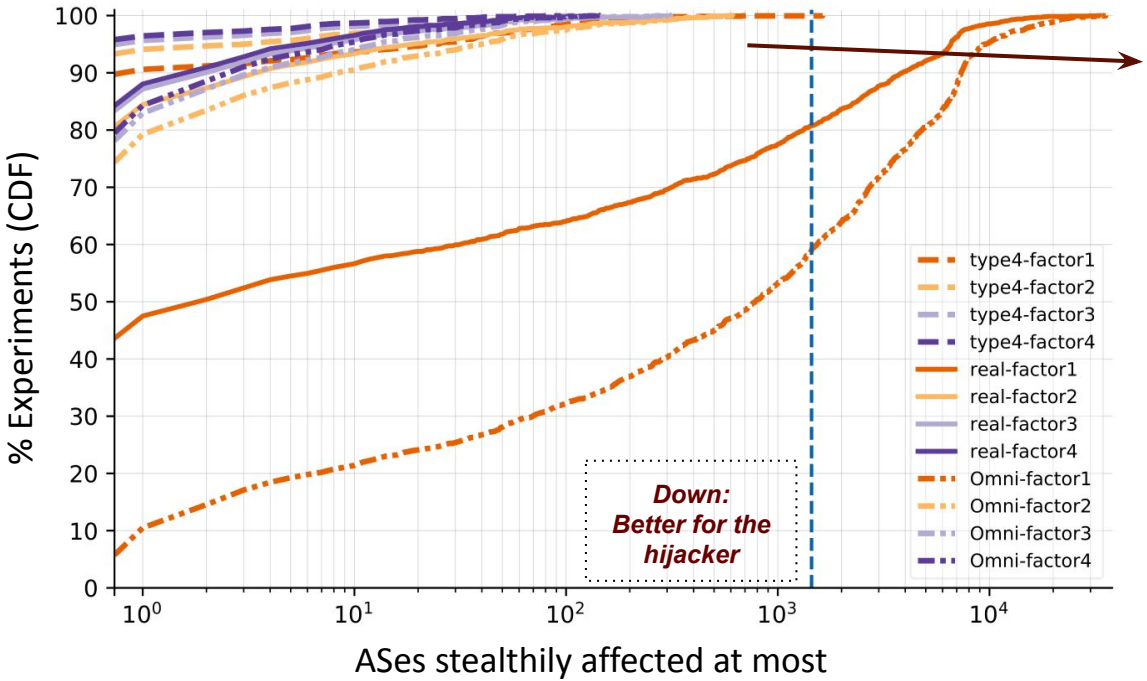
- **Type-1: 0.7% affected ASes**
- **Realistic: 16.2% affected ASes**
- **Omni: 23.5% affected ASes**

Fully IXP Topology (IXP100)

- **Type-1: 2.2% affected ASes**
- **Realistic: 45.5% affected ASes**
- **Omni: 49.0% affected ASes**

** Results based on the AS-level graph*

Appendix – Topologies With More Monitors

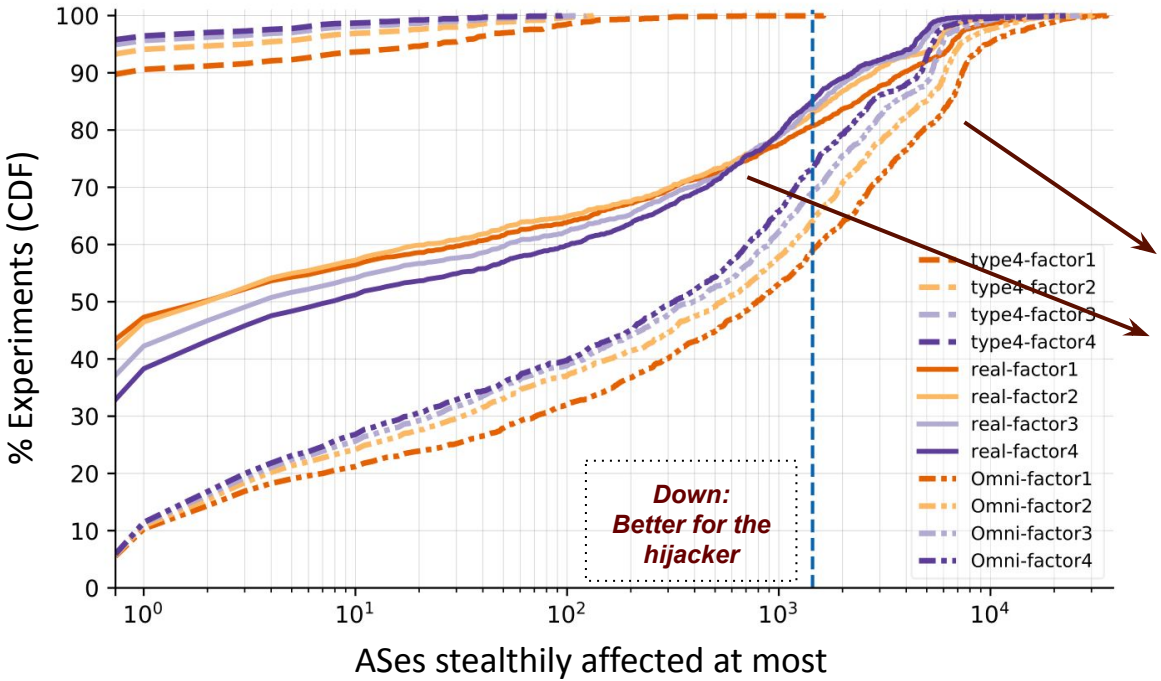


Non-Reactive Hijackers

- **Prevents attacks affecting > 2% Internet**

** Results based on the AS-level graph*

Appendix – Topologies With More Monitors



Non-Reactive Hijackers

- **Prevents attacks affecting > 2% Internet**

Reactive Hijackers

- **Realistic: 28.8% affected ASes down from 45.6%**
- **Omni: 31.8% affected ASes down from 49.0%**
- **Realistic Hijackers may benefit if < 800 ASes affected**

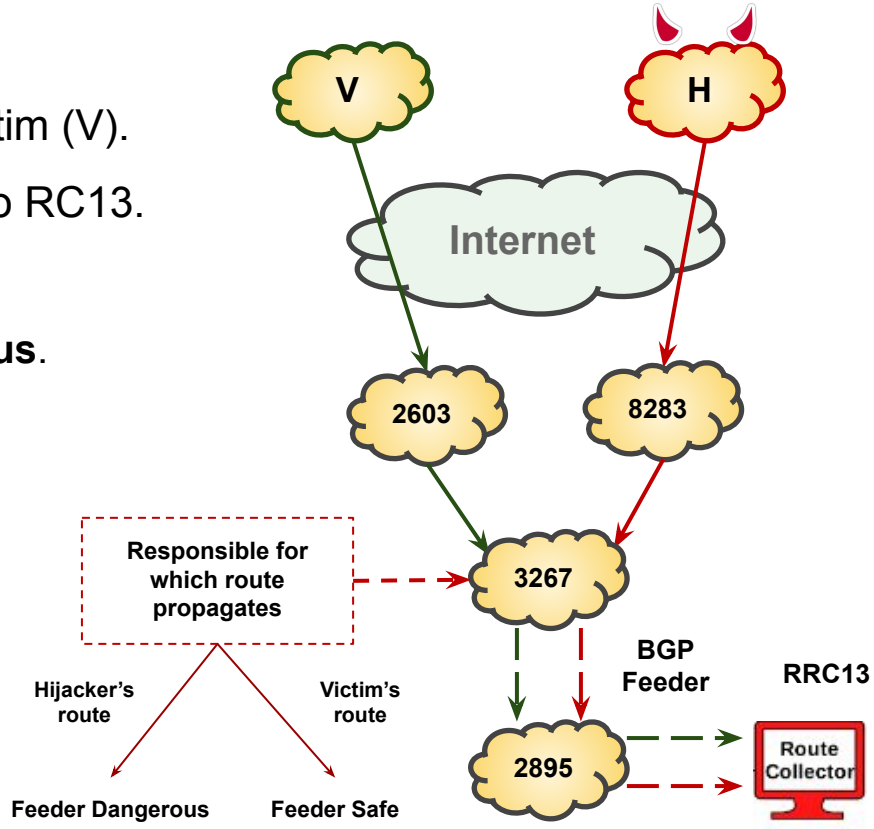
** Results based on the AS-level graph*

Classifying the Feeders: A Real World Example

- ➔ Hijacker (H) announces same prefix as Victim (V).
- ➔ AS3267 chooses which route propagates to RC13.
  - ◆ IF V route propagates: Feeder **safe**.
  - ◆ IF H route propagates: Feeder **dangerous**.

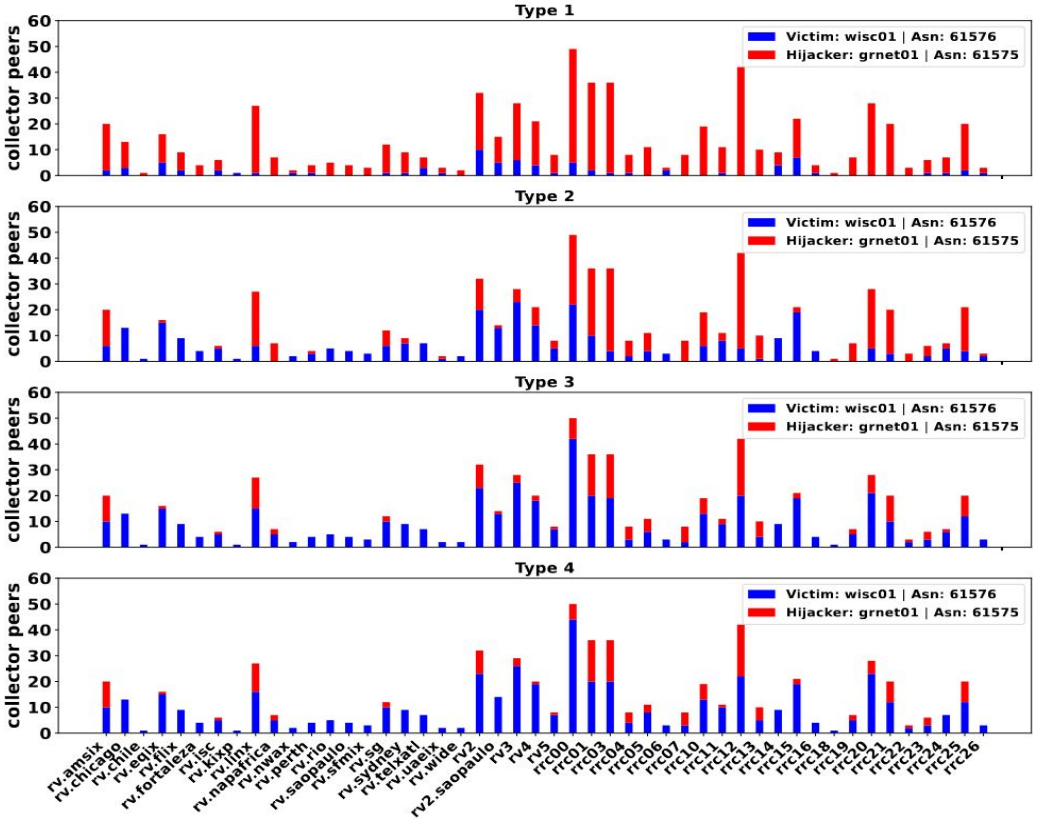
Classifiers Tested:

- ❖ A Proximity Classifier (AS-path lengths).
- ❖ A business relationship Classifier (Gao-Rexford).



Real World: PEERING Testbed

- How the hijack visibility changes (per RC) by announcing less-preferred hijacks.
  - **Type-0**: { **ASH** }
  - **Type-1**: { **ASH**, **ASV** }
  - **Type-N**: { **ASH**, **…**, **ASV** }



Proximity Classifier – Reason for Misclassifications

Proximity Classifier: Reason for Misclassification (FP / FN)	GRnet Transit ASN 5408	AMS Transit ASN 8283	AMS Transit ASN 12859	AMS Peer ASN 9002	AMS Peer ASN 6461	AMS Peer ASN 52320
1. Shortest AS-Path Violation	**FP: 1 FN: 140**	**FP: 2 FN: 158**	**FP: 0 FN: 79**	**FP: 0 FN: 0**	**FP: 1 FN: 8**	**FP: 0 FN: 0**
a) Longer Path preferred	*FP: 0 FN: 139*	*FP: 1 FN: 157*	*FP: 0 FN: 79*	*FP: 0 FN: 0*	*FP: 1 FN: 0*	*FP: 0 FN: 0*
b) Victim Path not observed	*FP: 1 FN: 0*	*FP: 1 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*
c) Hijacker Path not observed	*FP: 0 FN: 1*	*FP: 0 FN: 1*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 8*	*FP: 0 FN: 0*
3. Tie breakers Violations	**FP: 2 FN: 0**	**FP: 15 FN: 0**	**FP: 29 FN: 0**	**FP: 15 FN: 0**	**FP: 33 FN: 0**	**FP: 1 FN: 0**
d) Victim path preferred	*FP: 2 FN: 0*	*FP: 15 FN: 0*	*FP: 29 FN: 0*	*FP: 15 FN: 0*	*FP: 33 FN: 0*	*FP: 1 FN: 0*
Total (FP / FN)	**FP: 3 FN: 140**	**FP: 17 FN: 158**	**FP: 29 FN: 79**	**FP: 15 FN: 0**	**FP: 34 FN: 8**	**FP: 1 FN: 0**

Gao-Rexford Classifier – Reason for Misclassifications

Gao Rexford Classifier Reason for Misclassification (FP / FN)	GRnet Transit ASN 5408	AMS Transit ASN 8283	AMS Transit ASN 12859	AMS Peer ASN 9002	AMS Peer ASN 6461	AMS Peer ASN 52320
1. Gao Rexford Violation	**FP: 52 FN: 0**	**FP: 27 FN: 0**	**FP: 48 FN: 0**	**FP: 3 FN: 0**	**FP: 2 FN: 0**	**FP: 1 FN: 0**
a) customer - provider	*FP:1 FN:0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*
b) customer - peer	*FP: 0 FN: 0*	*FP: 6 FN: 0*	*FP: 20 FN:0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*
c) peer - provider	*FP: 51 FN: 0*	*FP: 21 FN: 0*	*FP: 28 FN:0*	*FP: 3 FN: 0*	*FP: 2 FN: 0*	*FP: 1 FN: 0*
2. Shortest AS-Path Violation	**FP: 1 FN: 8**	**FP: 2 FN: 17**	**FP: 0 FN: 9**	**FP: 0 FN: 0**	**FP: 1 FN: 8**	**FP: 0 FN: 0**
d) Longer Path preferred (Same Gao relation)	*FP:0 FN: 4*	*FP: 0 FN: 13*	*FP: 0 FN: 9*	*FP: 0 FN: 0*	*FP: 1 FN: 0*	*FP: 0 FN: 0*
e) Longer Path preferred (Unknown relation)	*FP: 0 FN: 3*	*FP: 1 FN: 3*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*
f) Victim Path not observed	*FP: 1 FN: 0*	*FP: 1 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 0*
g) Hijacker Path not observed	*FP: 0 FN: 1*	*FP: 0 FN: 1*	*FP: 0 FN: 0*	*FP: 0 FN: 0*	*FP: 0 FN: 8*	*FP: 0 FN: 0*
3. Tie breakers Violations	**FP: 2 FN: 0**	**FP: 8 FN: 0**	**FP: 17 FN: 0**	**FP: 15 FN: 0**	**FP: 33 FN: 0**	**FP: 1 FN: 0**
h) Victim path preferred	*FP: 2 FN: 0*	*FP: 8 FN: 0*	*FP: 17 FN: 0*	*FP: 15 FN: 0*	*FP: 33 FN: 0*	*FP: 1 FN: 0*
Total (FP / FN)	**FP: 55 FN: 8**	**FP: 37 FN: 17**	**FP: 65 FN: 9**	**FP: 18 FN: 0**	**FP: 36 FN: 8**	**FP: 2 FN: 0**

More Results

- For more experiment results: Refer to our *Published Journal*.