BGP Hijackers That Evade Public Route Collectors

RIPE SEE 11 Meeting: Split, Croatia

Alexandros Milolidakis
miloli@kth.se

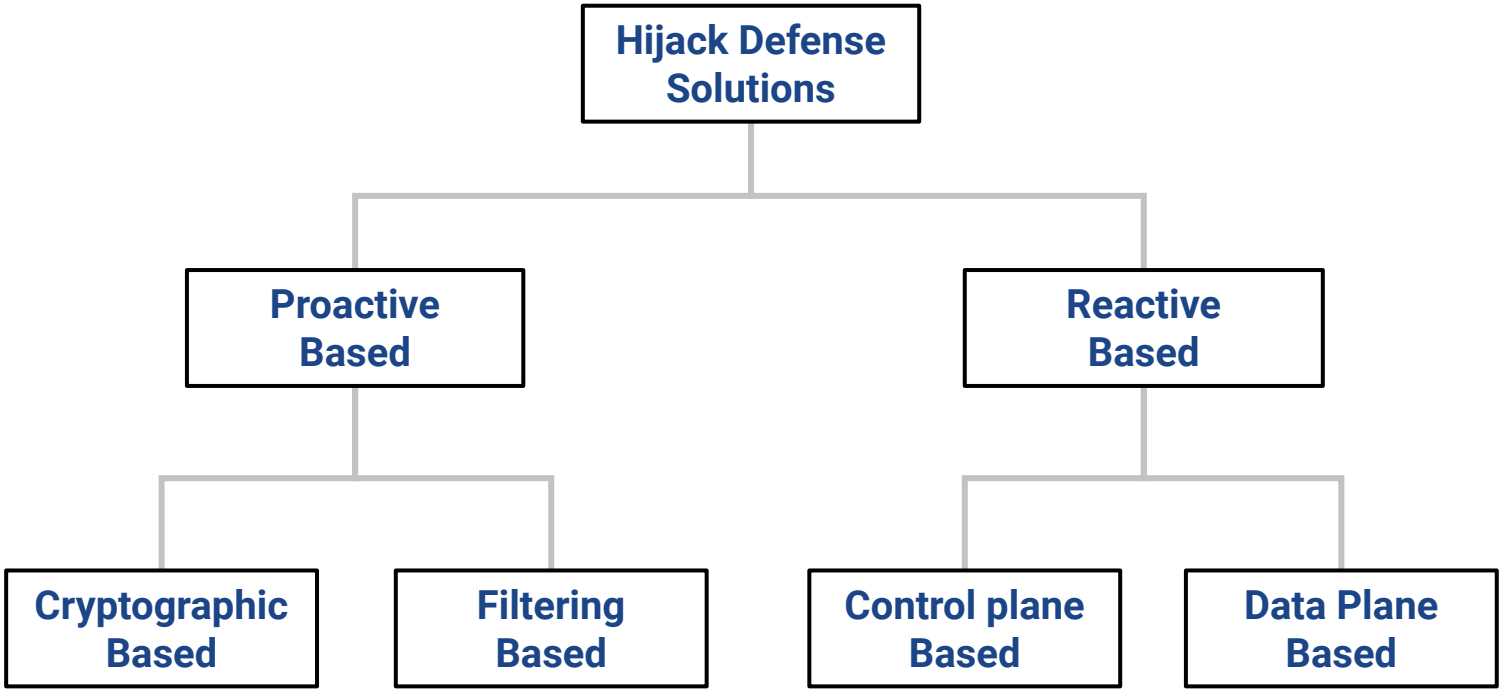
BGP Prefix Hijacking

Documented Suspicious BGP Hijacks:

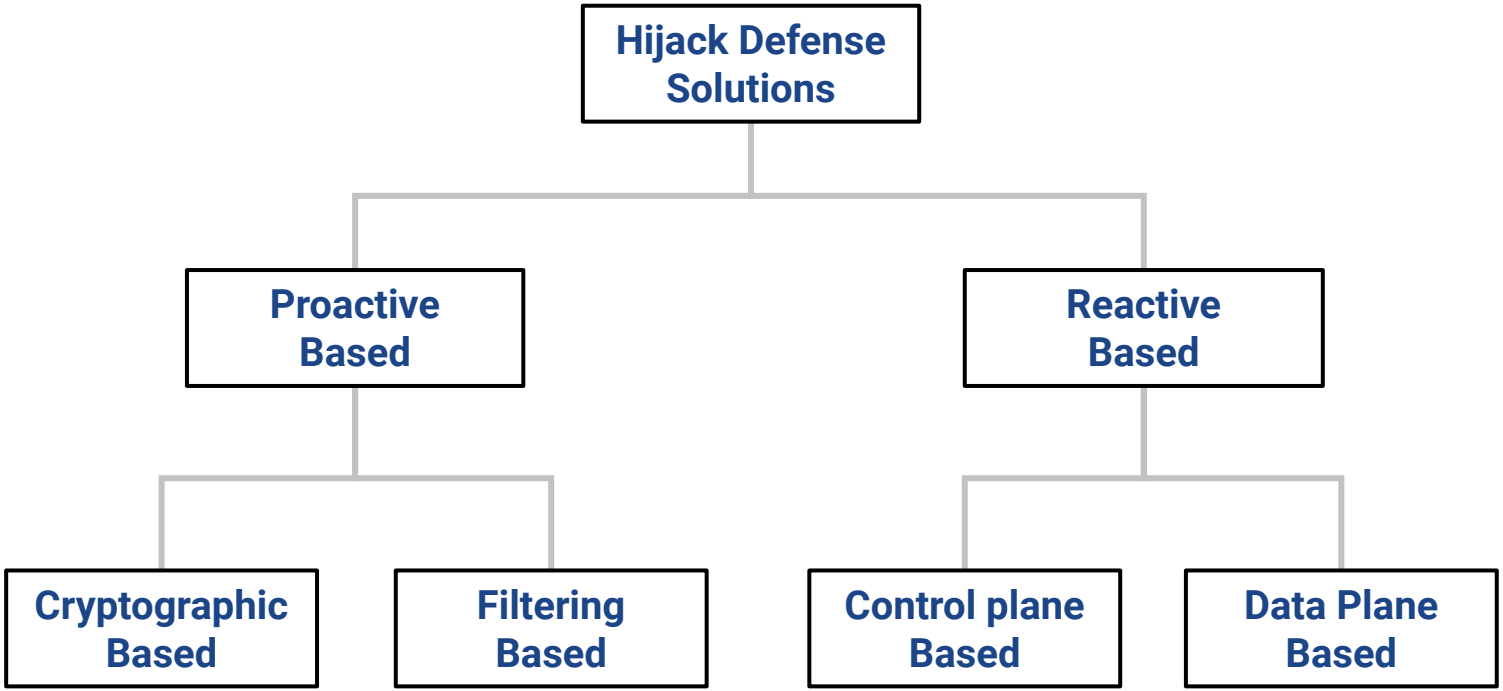
- Targets 2022: Governmental infrastructure **[1],** Cryptocurrency services **[2],** etc.
- Incidents 2021: 775 suspicious BGP hijacks **[3]**.
- Incidents 2020: 2255 suspicious BGP hijacks **[4]**.
- Incidents 2019: 1727 suspicious BGP hijacks **[4]**.

[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

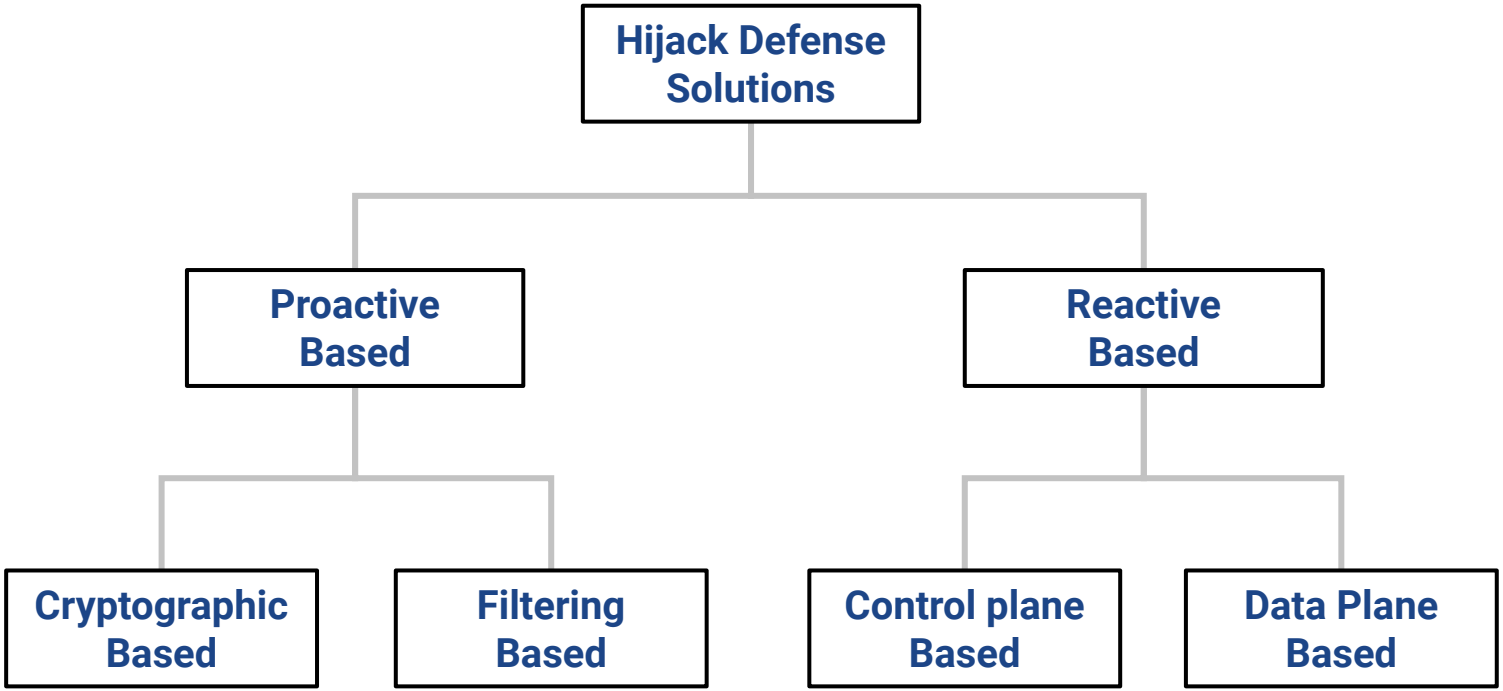


Current Solutions



Not Sufficient for all forms of hijacks

Current Solutions



Current Hijack Solutions

★ Current Commercial solutions rely on *Route collectors* & *Looking Glasses*.

Route Collectors (RC):

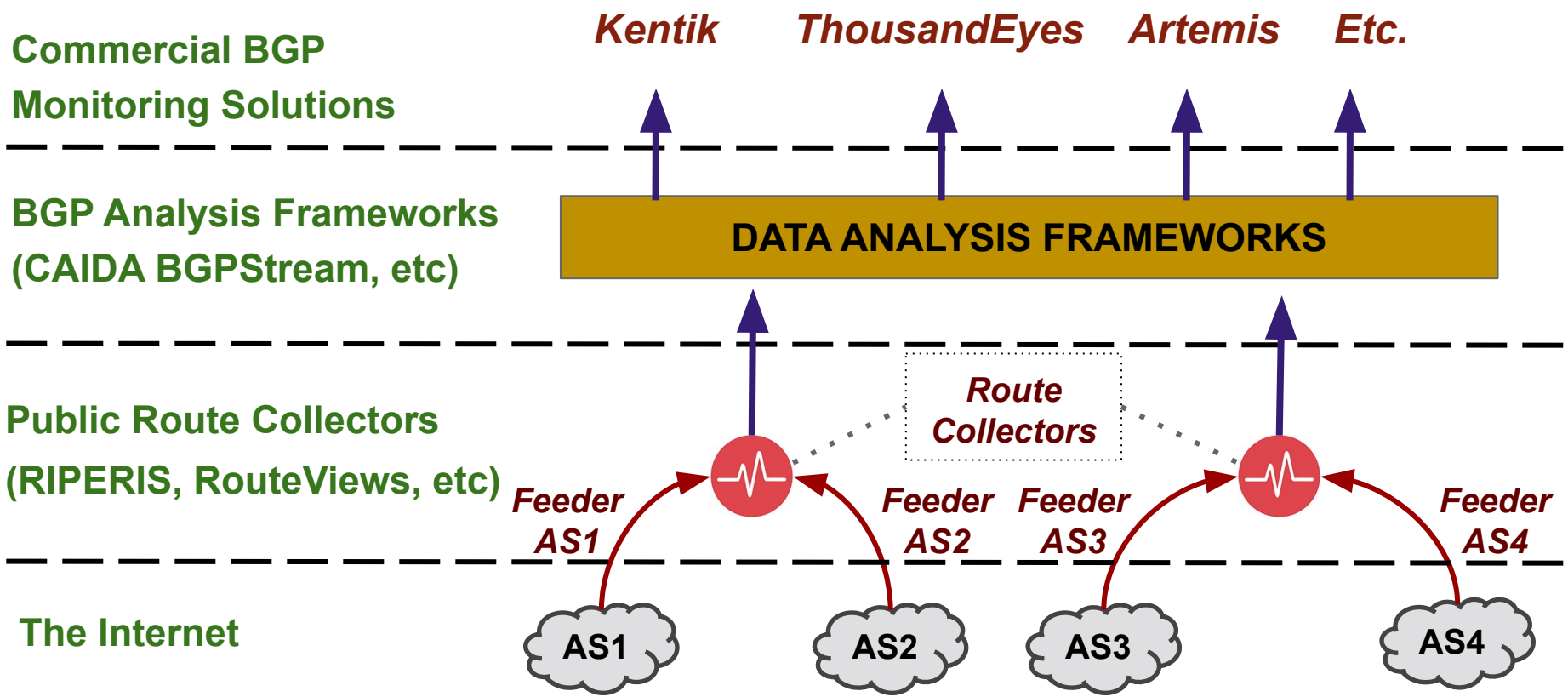
❖ BGP speaking devices that collect & report routes received from their neighbors.

Public Route Collector Infrastructure:

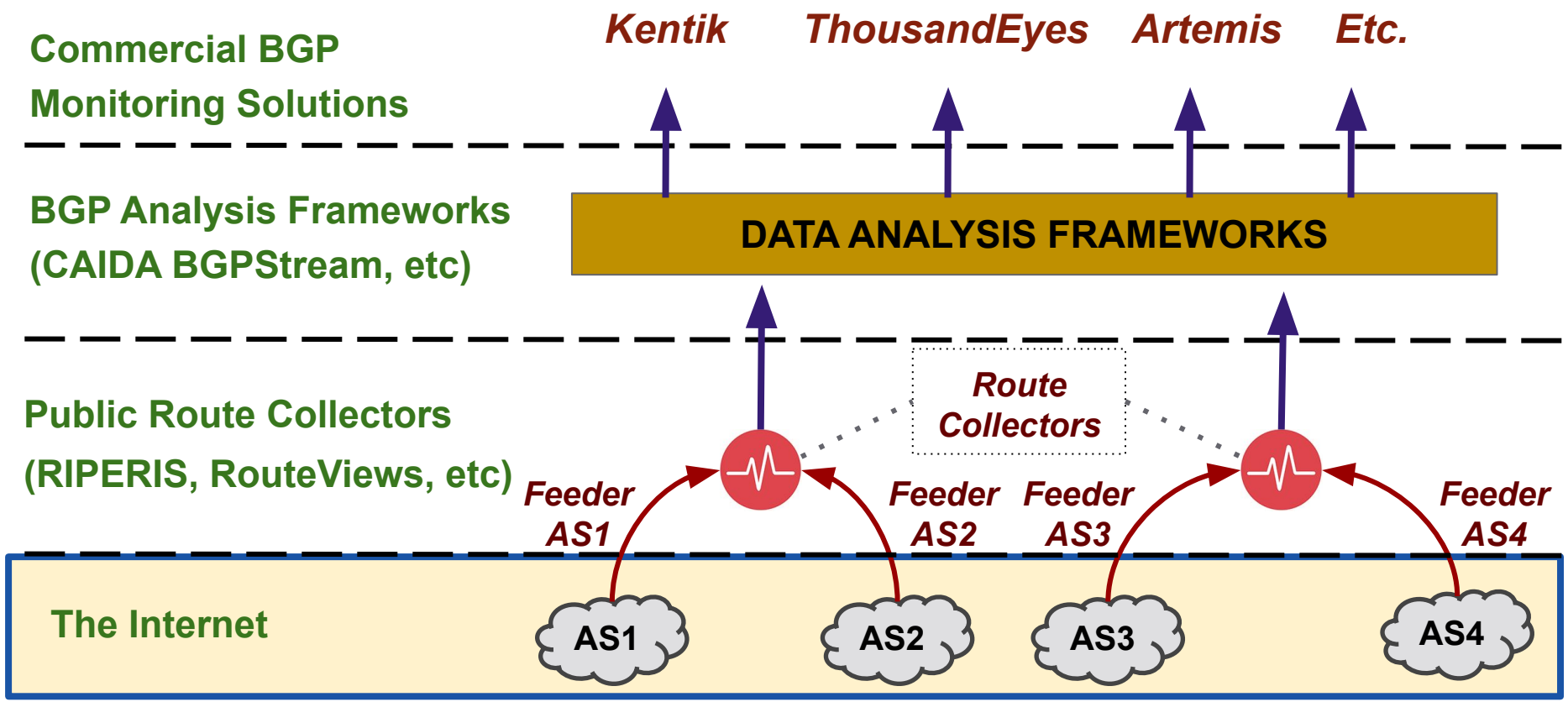
❖ Namely: RIPE-RIS and Routeviews.

❖ Collection of multiple route collectors distributed around the world.

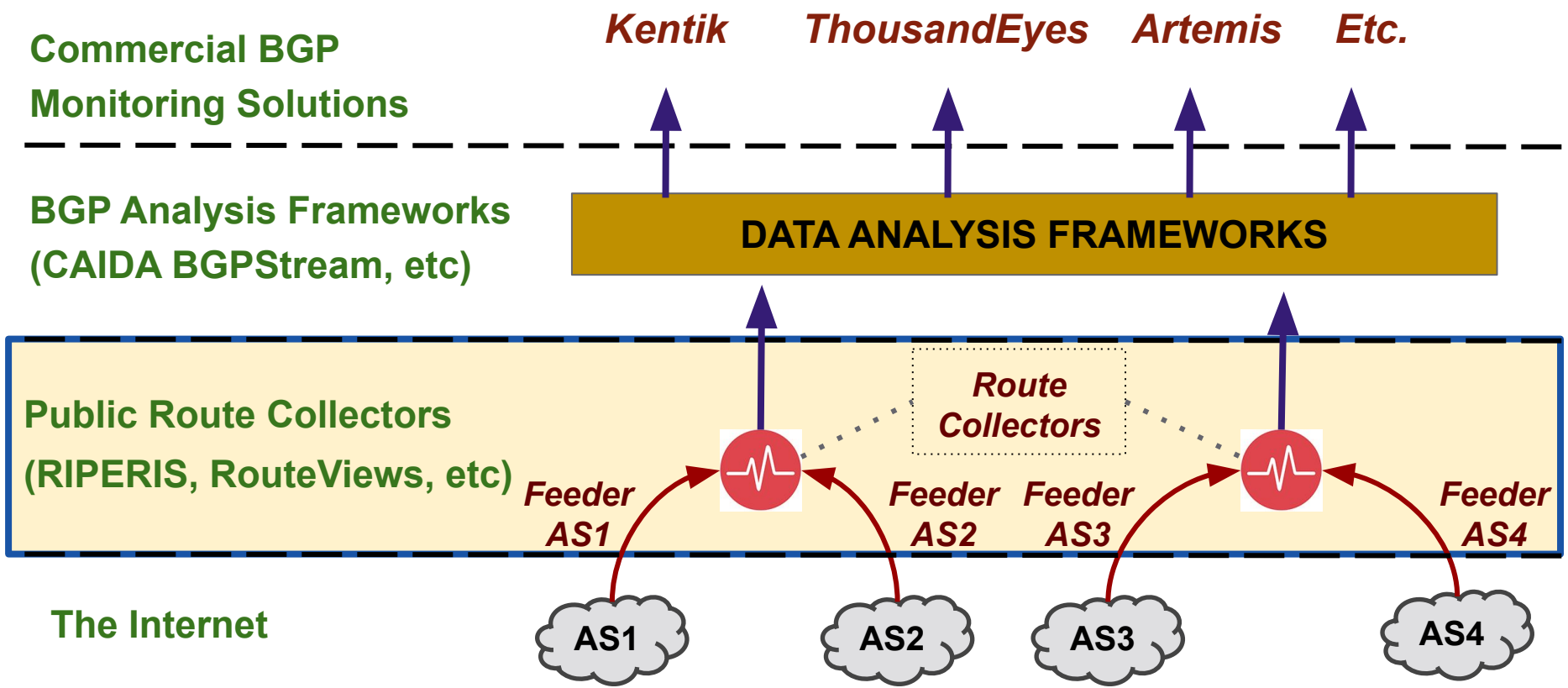
Pipeline: Route Collection by Commercial Solutions



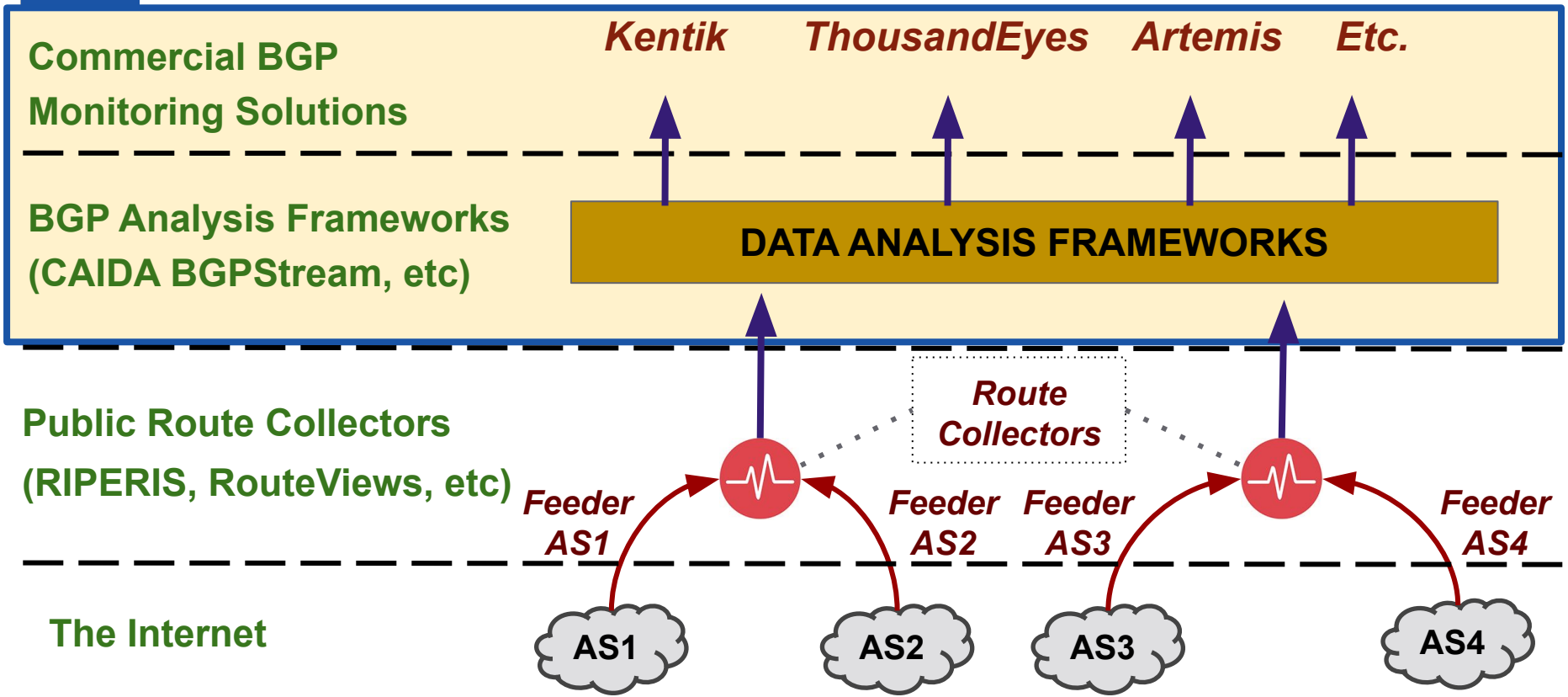
Pipeline: Route Collection by Commercial Solutions



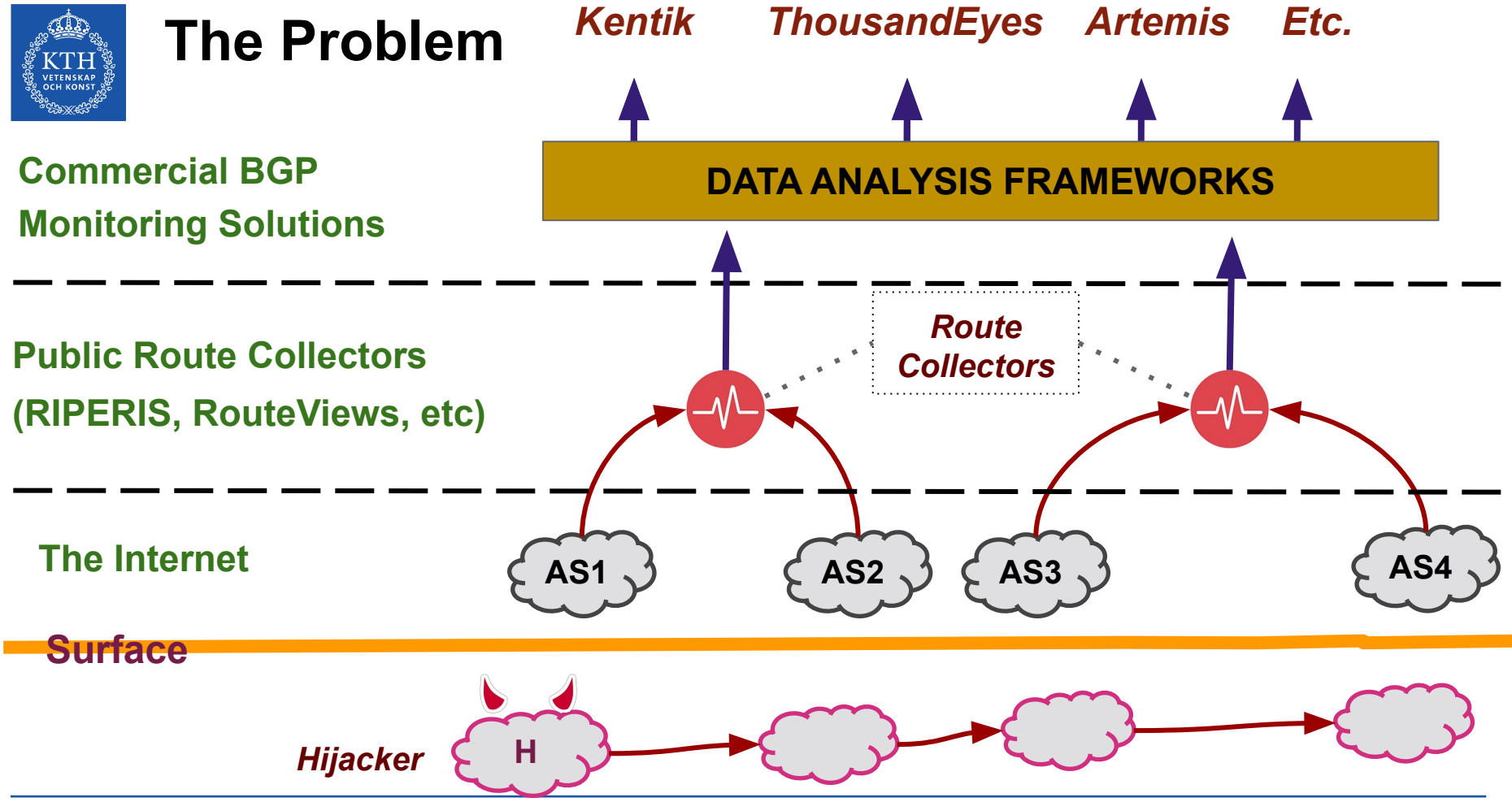
Pipeline: Route Collection by Commercial Solutions



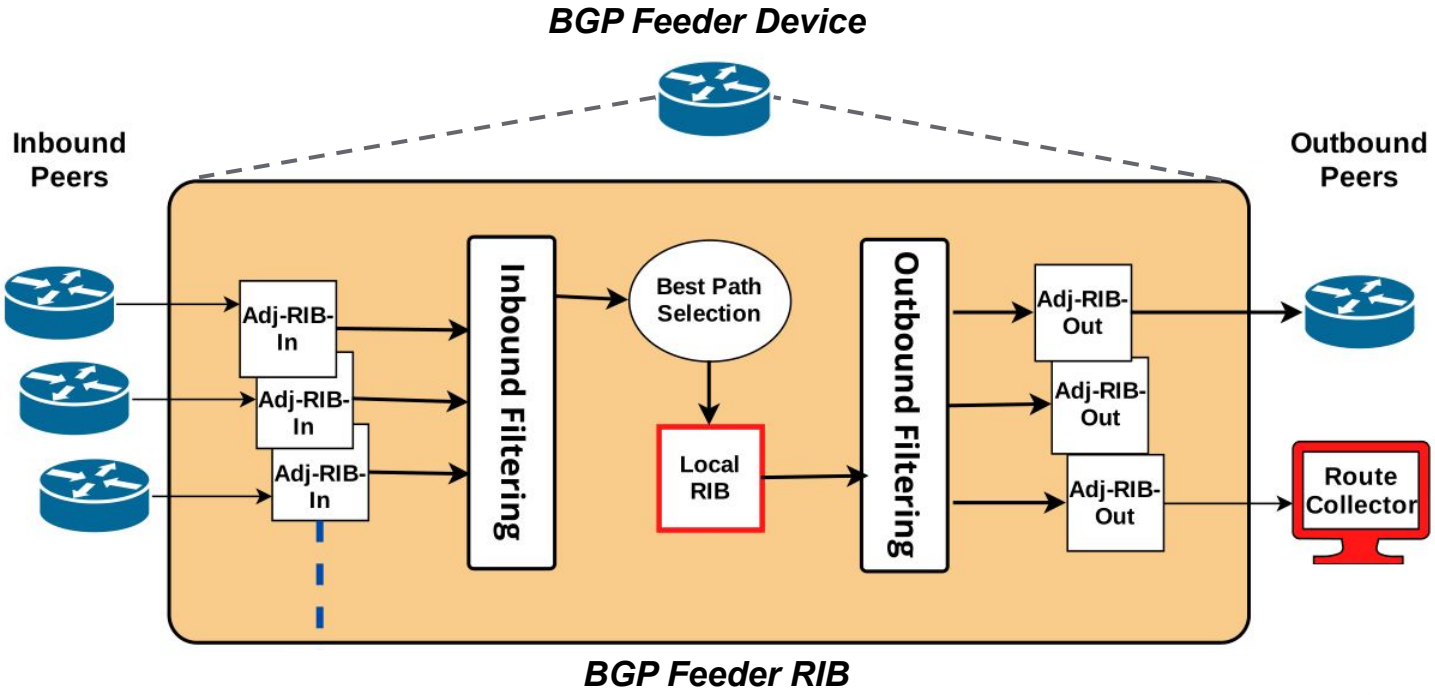
Pipeline: Route Collection by Commercial Solutions



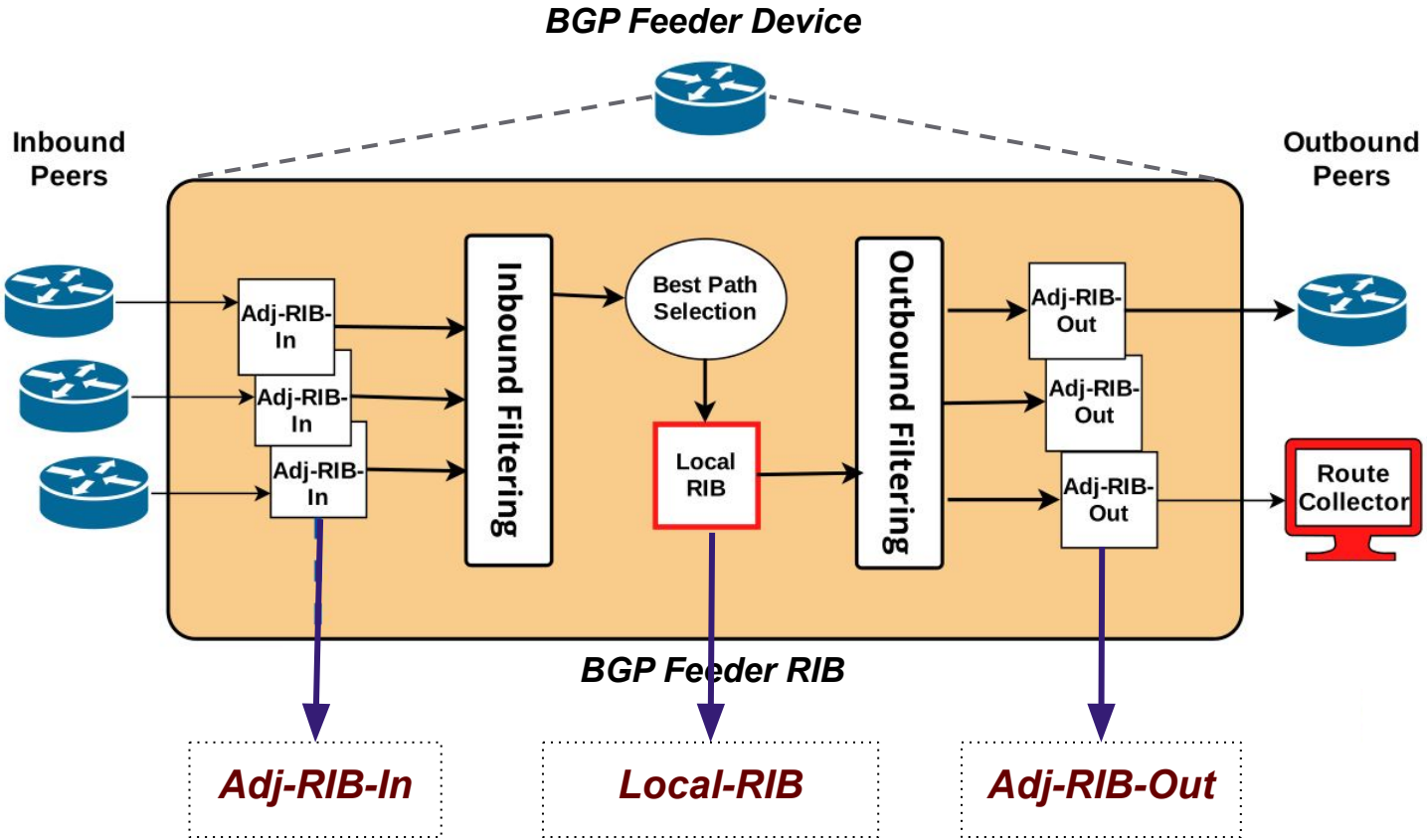
The Problem


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

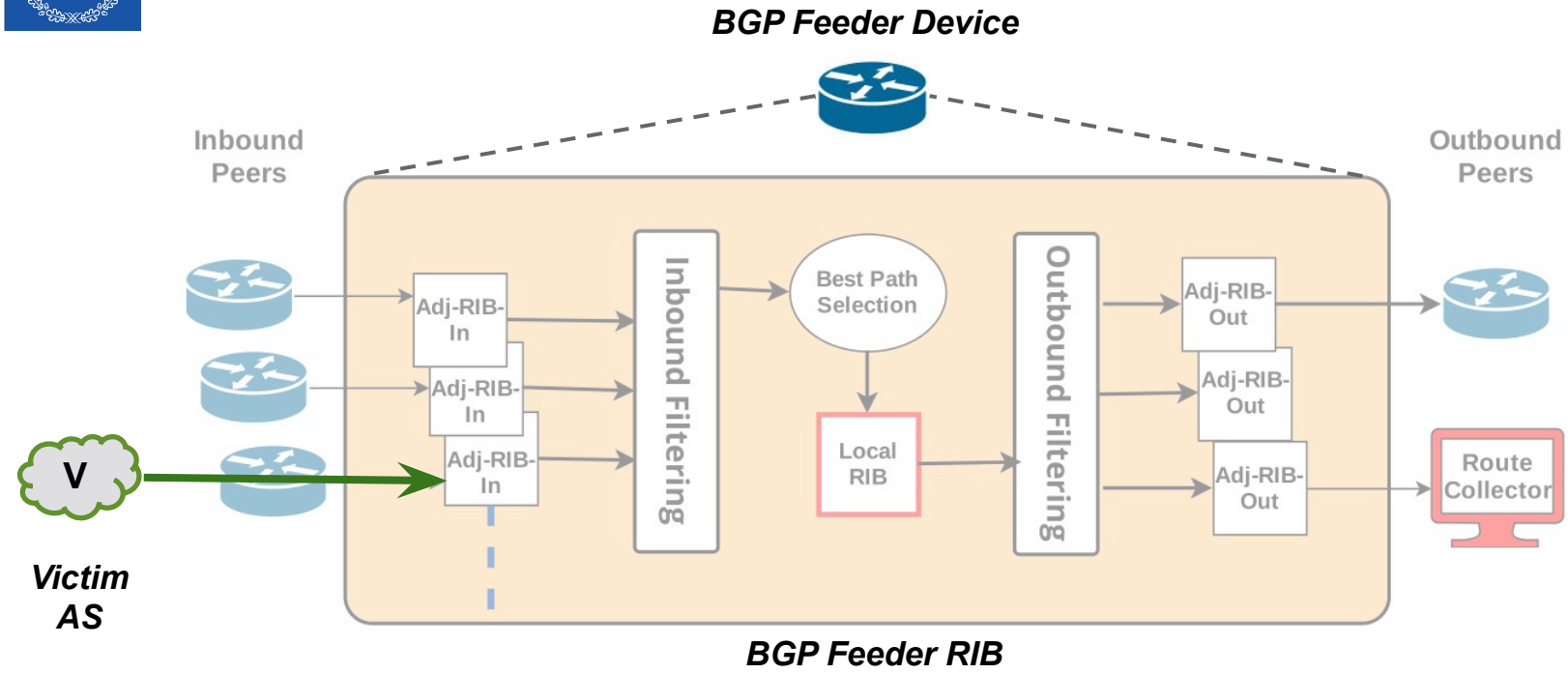
The Problem: Example of Stealthy Hijack to RC



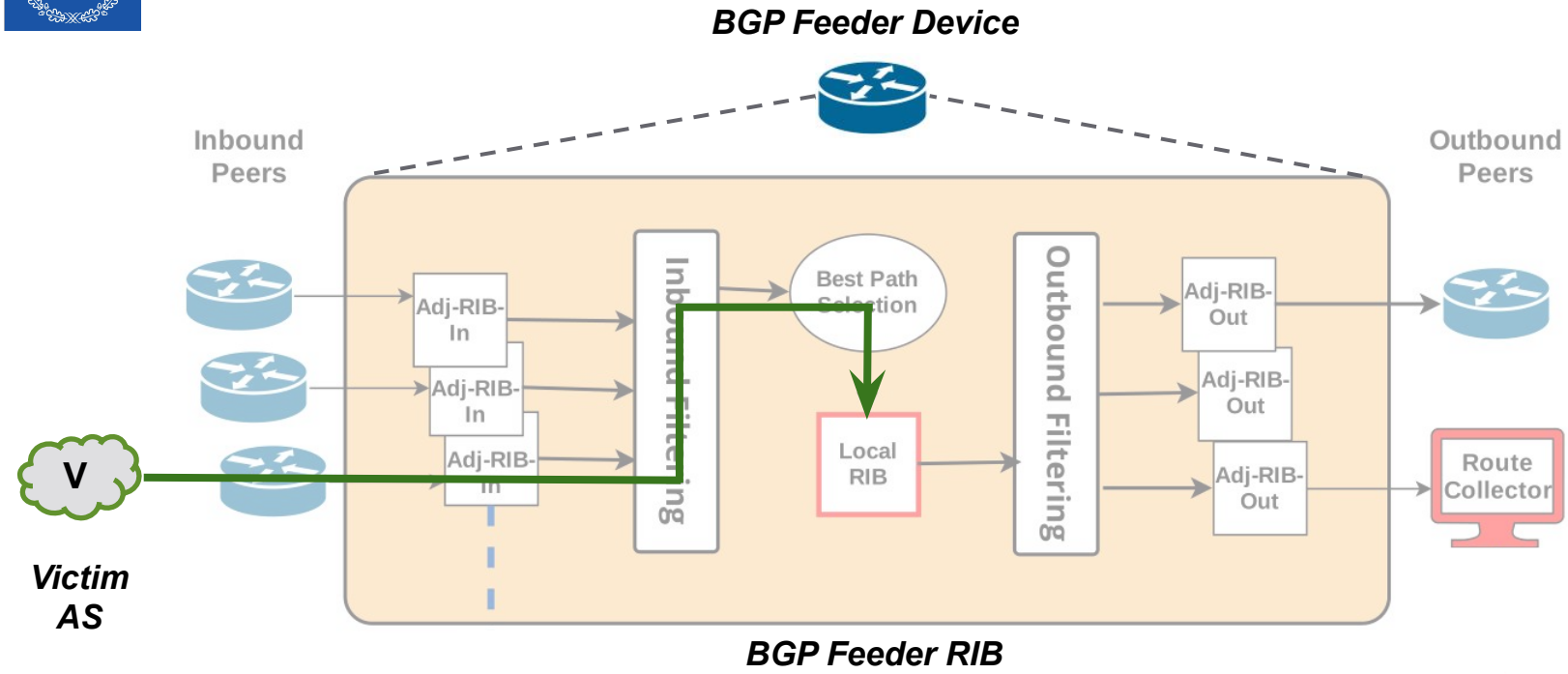
The Problem: Example of Stealthy Hijack to RC



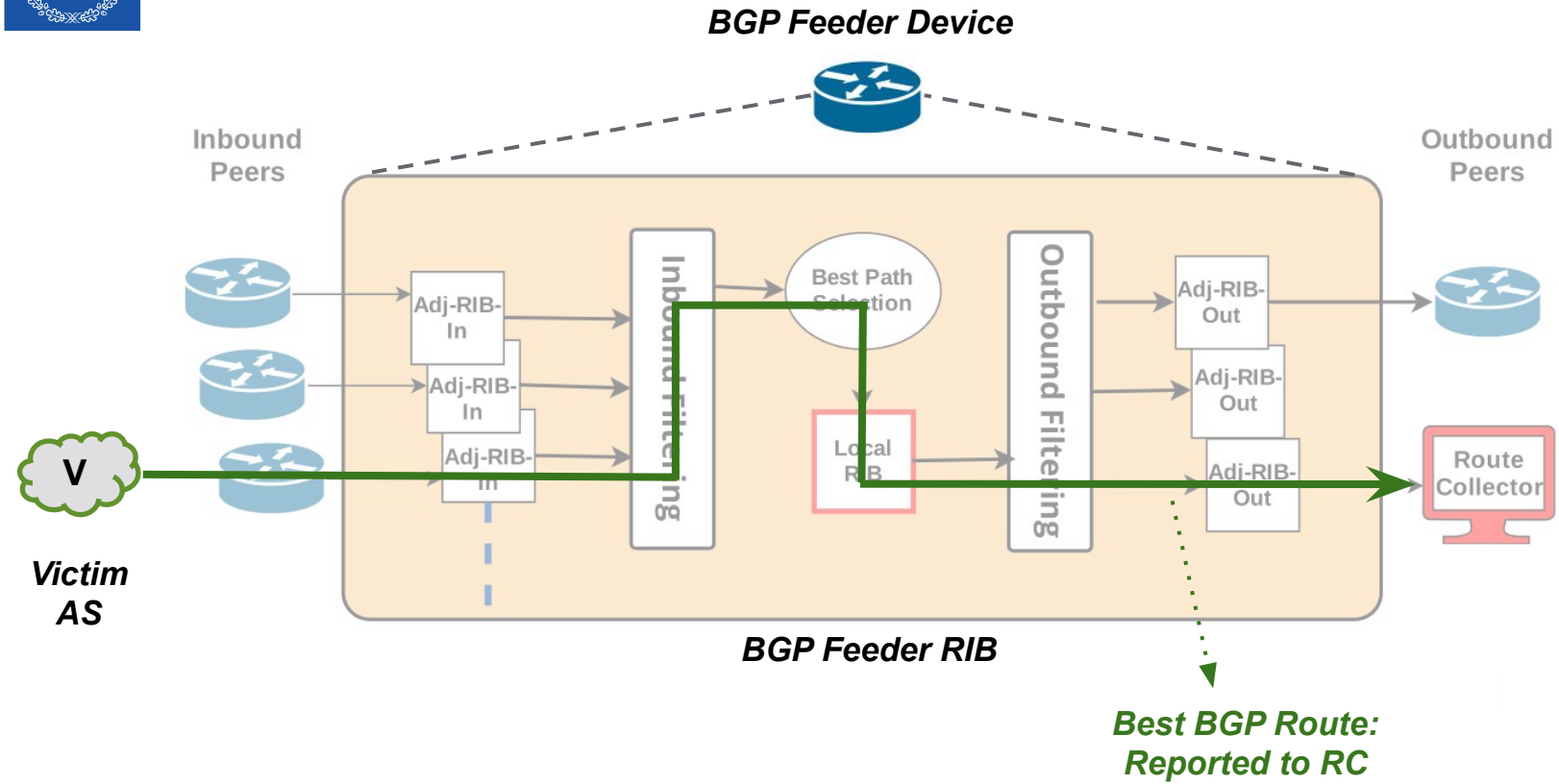
The Problem: Example of Stealthy Hijack to RC



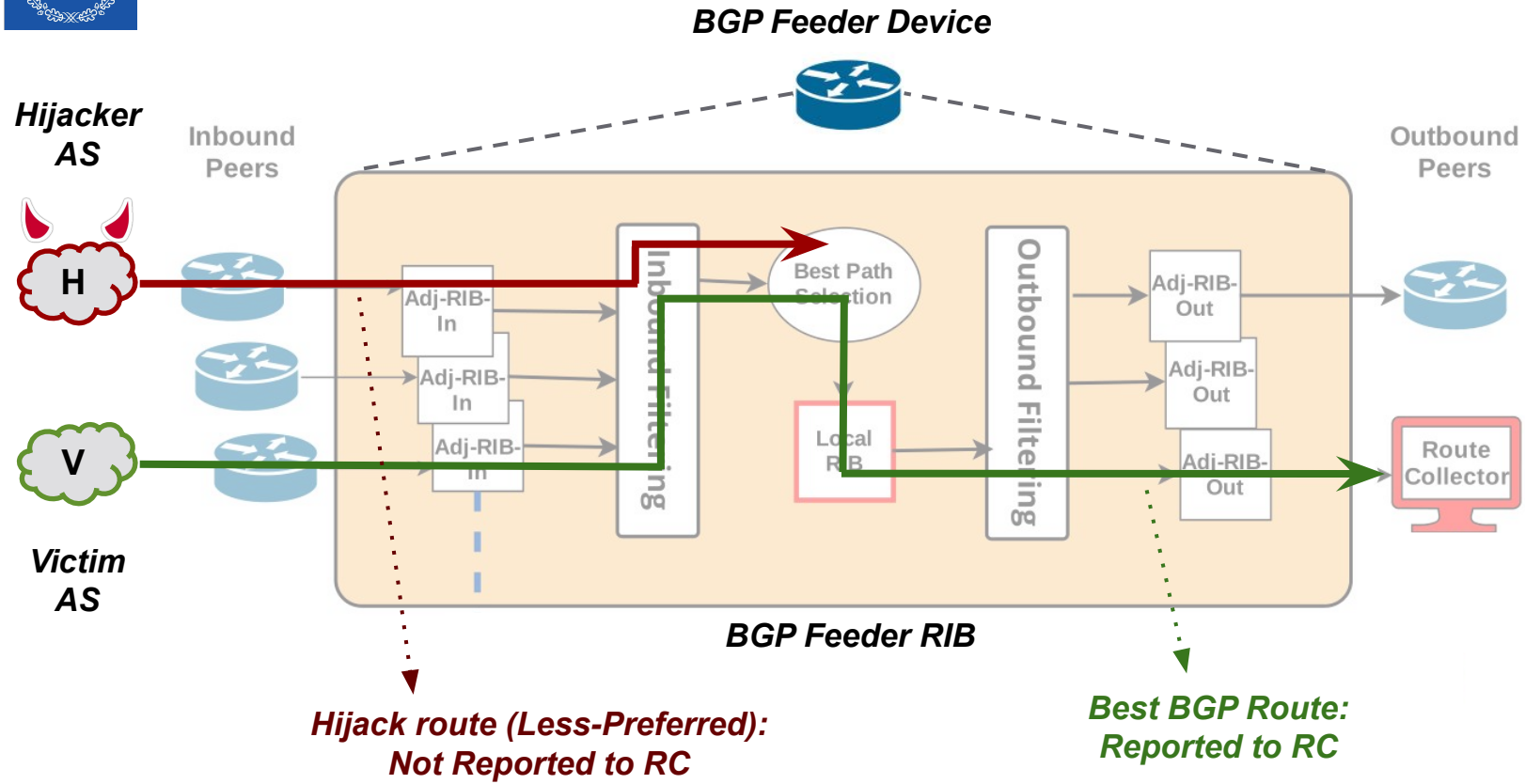
The Problem: Example of Stealthy Hijack to RC



The Problem: Example of Stealthy Hijack to RC



The Problem: Example of Stealthy Hijack to RC



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.

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.

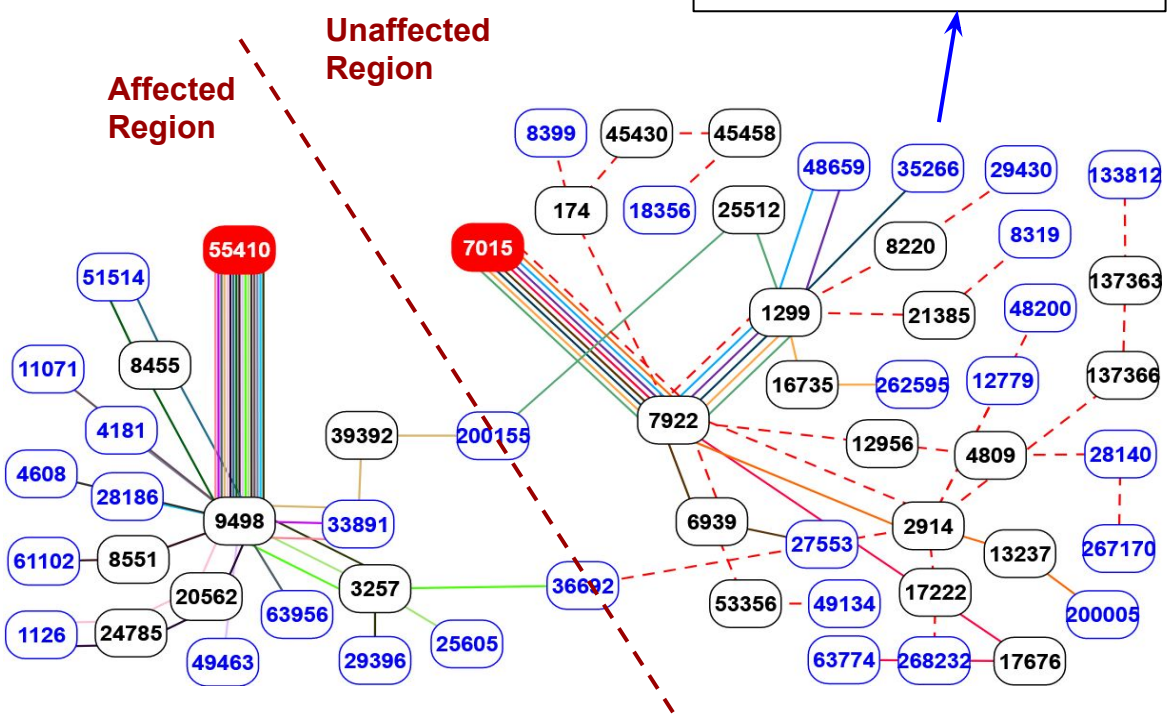


Fig: Vodafone (AS55410) leaking Comcast (AS7015) prefixes (16-04-21) (Source: Cisco BGPstream monitoring service)

What we Learned (2/3)

To design not observable hijacks by public RCs:

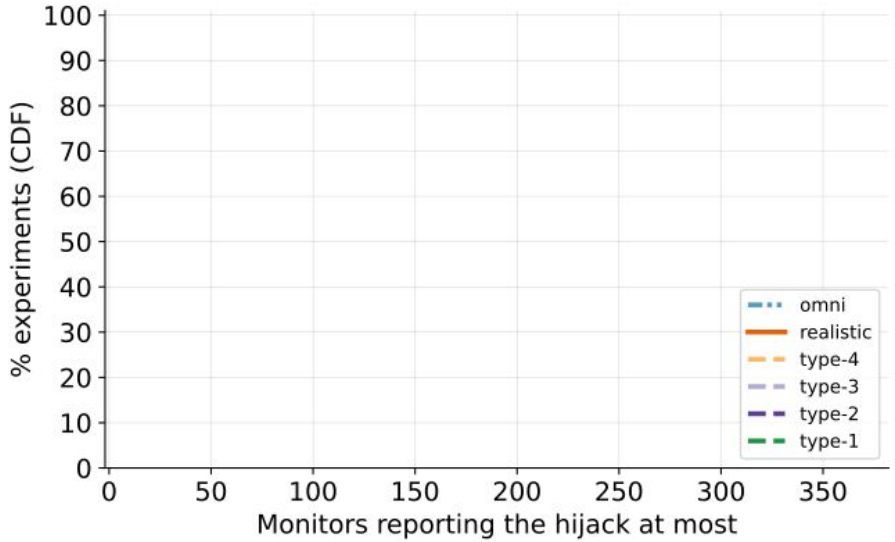
- Knowledge about which BGP feeders will report the attack matters.
- Knowledge about routing policies of other ASes matters.

What we Learned (2/3)

To design not observable hijacks by public RCs:

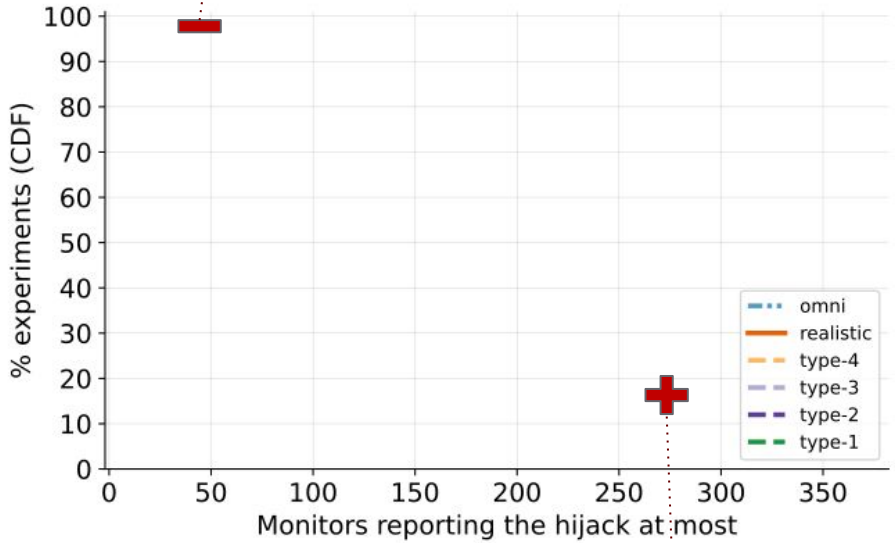
- Knowledge about which BGP feeders will report the attack matters.
- Knowledge about routing policies of other ASes matters.
  - *Baseline hijacker:* Traditional hijacker – does not deliberately avoid RCs.
  - *Realistic hijacker:* Limited knowledge inferred from routes public RCs disclose.
  - *Omniscient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

Knowledge Routing Policies Matters – Visibility



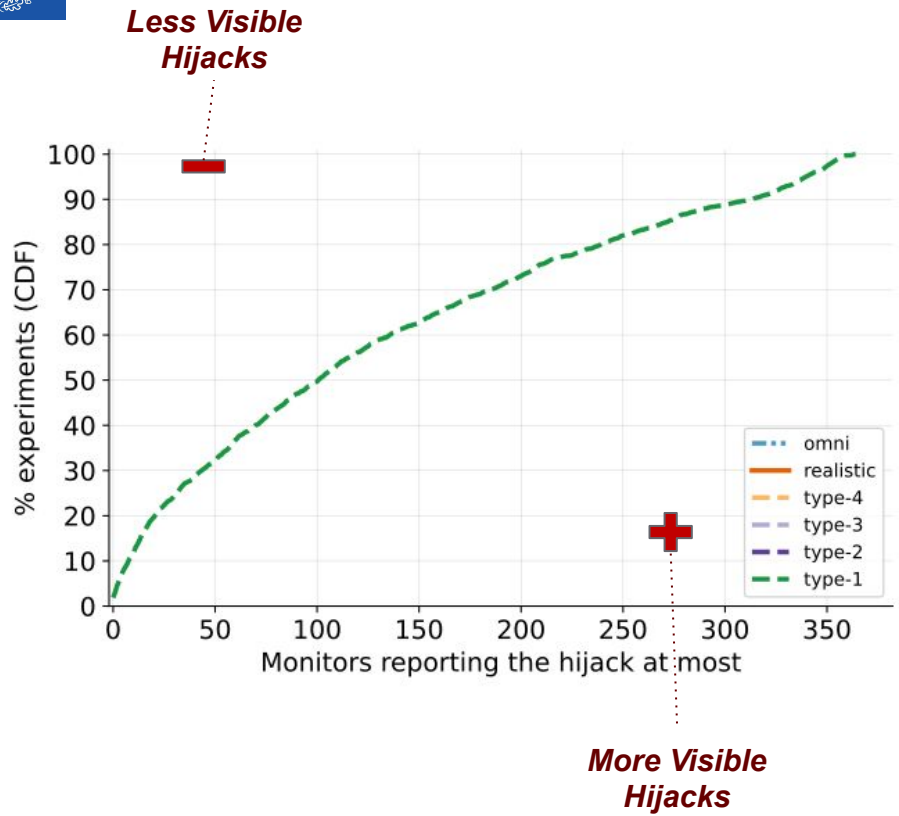
Knowledge Routing Policies Matters – Visibility

Less Visible Hijacks



More Visible Hijacks

Knowledge Routing Policies Matters – Visibility

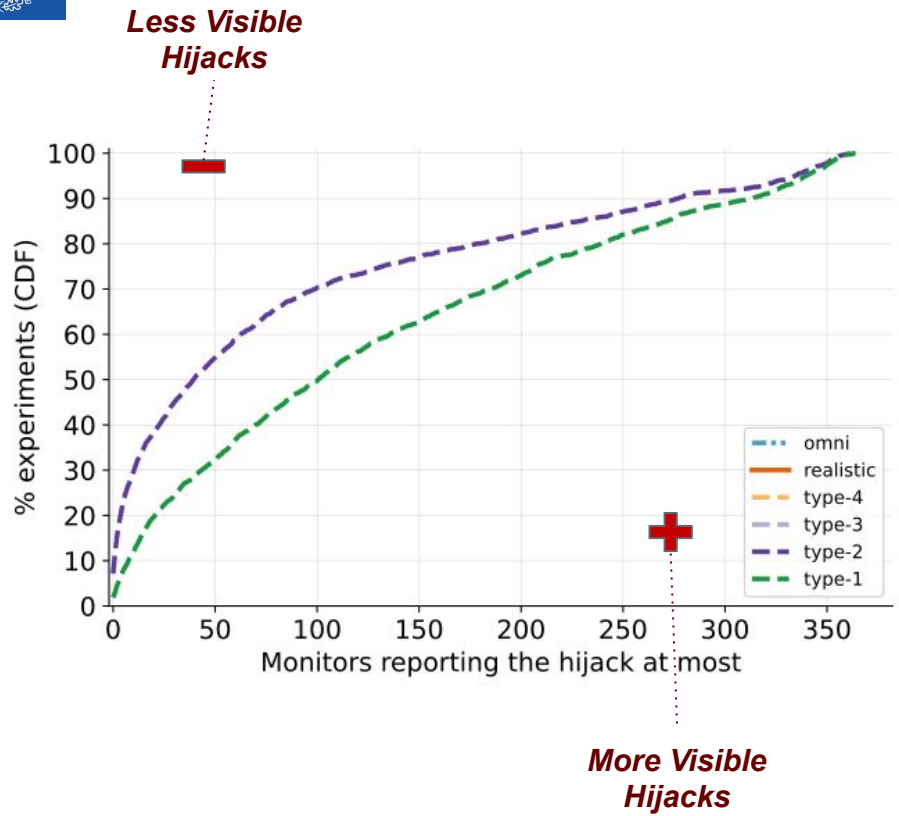


Baseline Hijackers (forged path shape):

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

Higher Type: *Longer* forged paths

Knowledge Routing Policies Matters – Visibility



Baseline Hijackers (forged path shape):

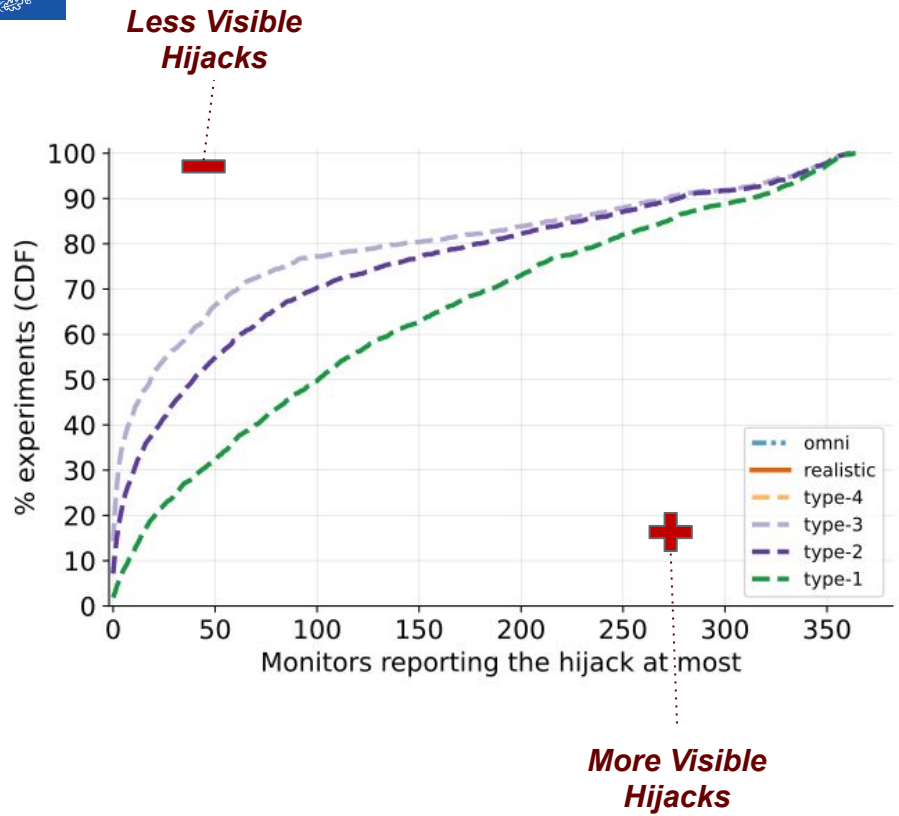
- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

Higher Type: *Longer* forged paths

Median Visibility

- **Type-1: 101 monitors**
- **Type-2: 40 monitors**
- **Type-3: 19 monitors**
- **Type-4: 10 monitors**

Knowledge Routing Policies Matters – Visibility



Baseline Hijackers (forged path shape):

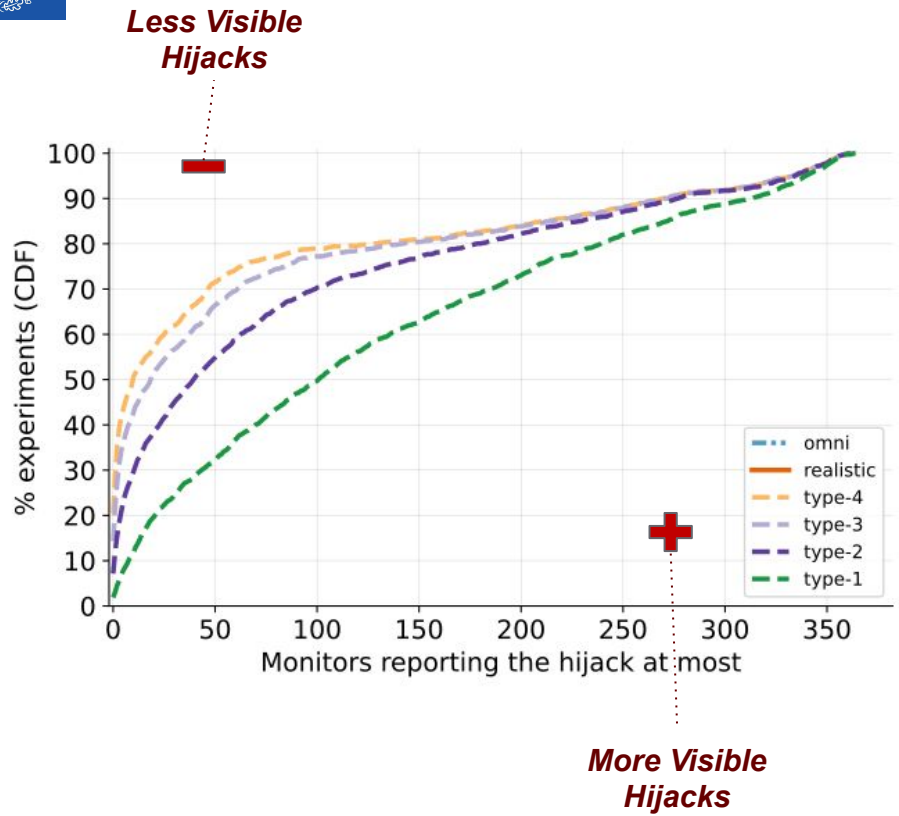
- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

Higher Type: *Longer* forged paths

Median Visibility

- **Type-1: 101 monitors**
- **Type-2: 40 monitors**
- **Type-3: 19 monitors**
- **Type-4: 10 monitors**

Knowledge Routing Policies Matters – Visibility



Baseline Hijackers (forged path shape):

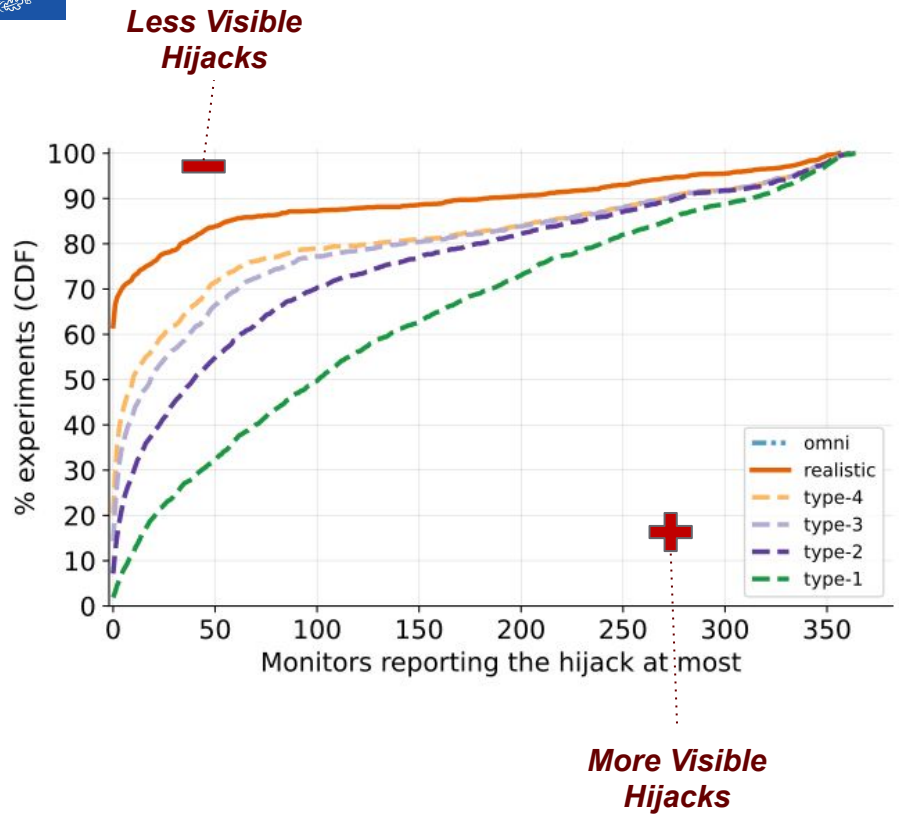
- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

Higher Type: *Longer* forged paths

Median Visibility

- **Type-1: 101 monitors**
- **Type-2: 40 monitors**
- **Type-3: 19 monitors**
- **Type-4: 10 monitors**

Knowledge Routing Policies Matters – Visibility



Baseline Hijackers (forged path shape):

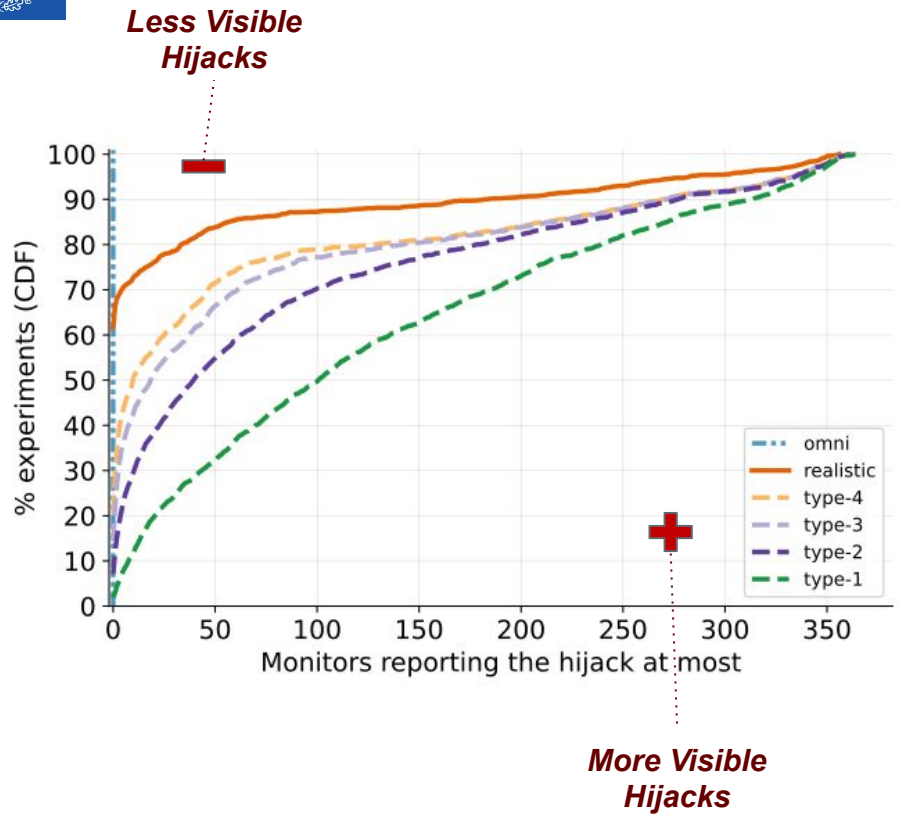
- **Type-0**: { **ASH** }
- **Type-1**: { **ASH**, **ASV** }
- **Type-N**: { **ASH**, **…**, **ASV** }

Higher Type: *Longer* forged paths

Realistic Hijackers:

- **Completely stealthy: 62% sims**
- **Less visible than baseline**
- **Shorter Type-4: 95% exported routes**

Knowledge Routing Policies Matters – Visibility



Baseline Hijackers (forged path shape):

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

Higher Type: *Longer* forged paths

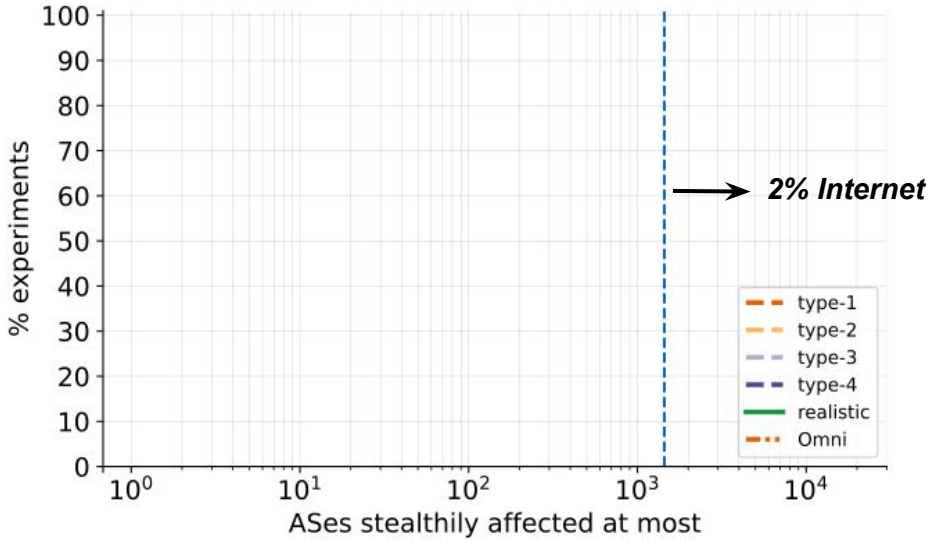
Realistic Hijackers:

- **Completely stealthy: 62% sims**
- **Less visible than baseline**
- **Shorter Type-4: 95% exported routes**

Omniscient Hijackers:

- **Completely stealthy**

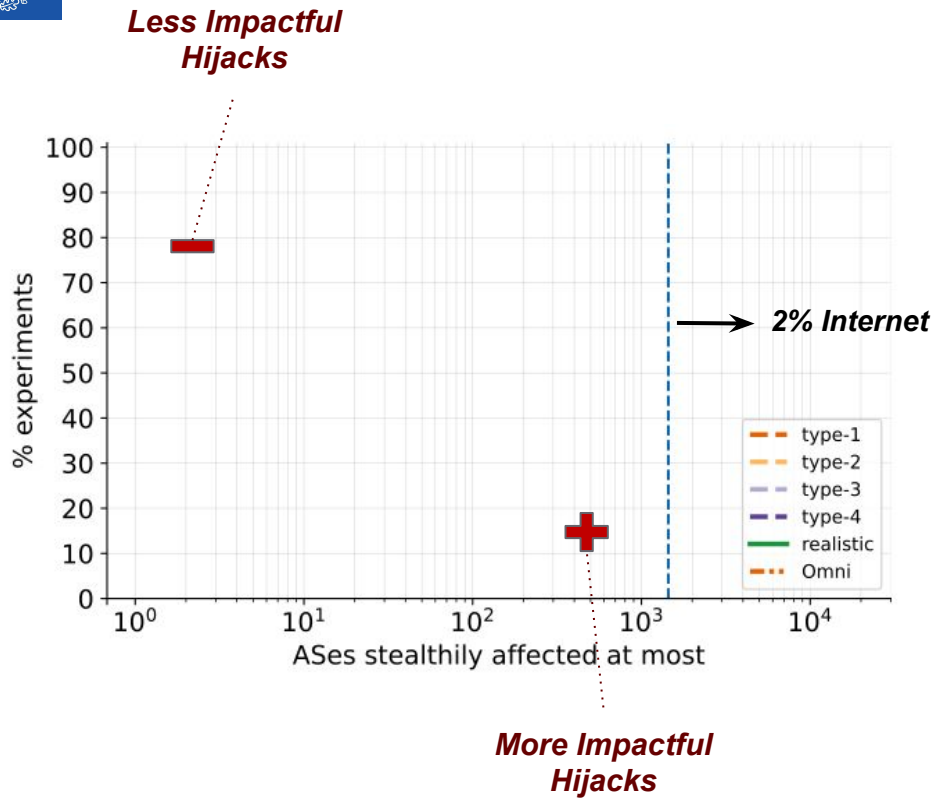
Knowledge Routing Policies Matters – Impact



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

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

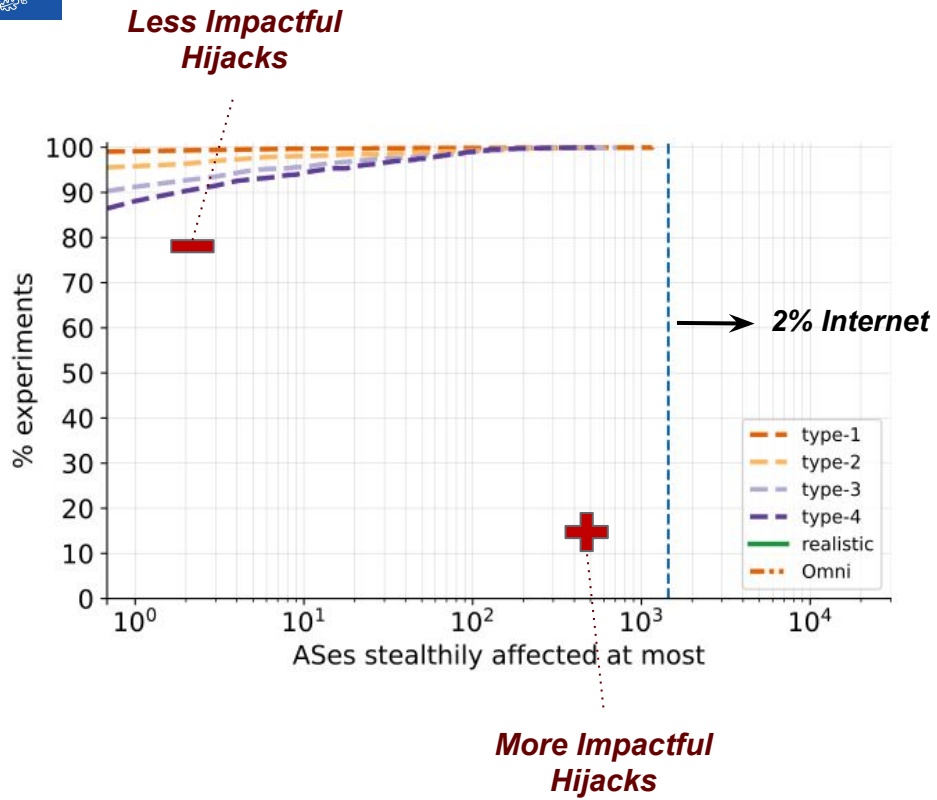
Knowledge Routing Policies Matters – Impact



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

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

Knowledge Routing Policies Matters – Impact



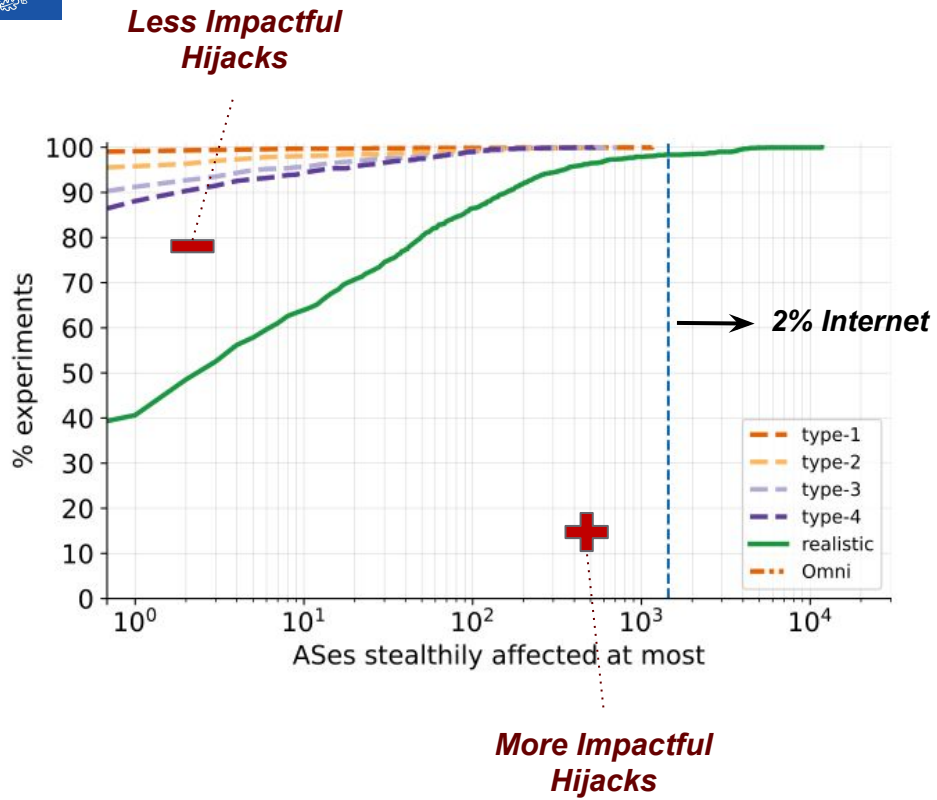
***Baseline Hijackers (forged path shape)*:**

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

Baseline Hijackers:

Cannot stealthily intercept > 2% Internet

Knowledge Routing Policies Matters – Impact



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

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

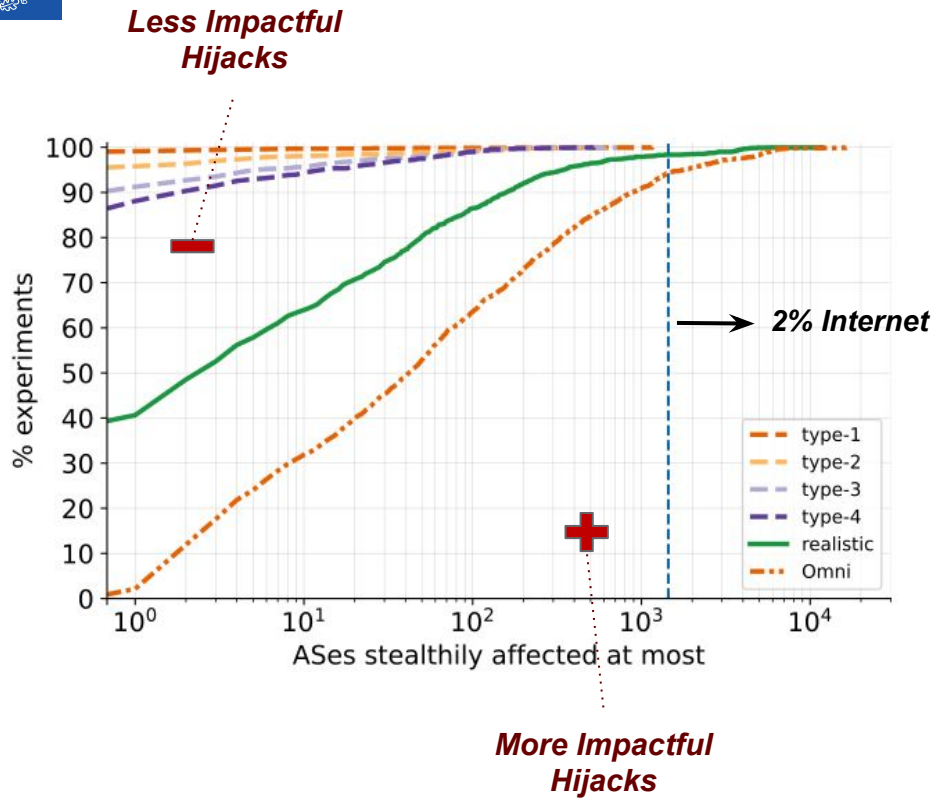
Baseline Hijackers:

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)**

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)**

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.

	Customers	***Peers***	***Transits***
Type-1			
Type-4			
Realistic			
Omni			

Table: Reason why forged routes were visible

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.

	Customers	***Peers***	***Transits***
Type-1	0.3%	47%	99%
Type-4			
Realistic			
Omni			

Table: Reason why forged routes were visible

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.

	Customers	***Peers***	***Transits***
Type-1	0.3%	47%	99%
Type-4	0.0%	24%	99%
Realistic			
Omni			

Table: Reason why forged routes were visible

Peers:

- **Path lengths matter more for such neighbors.**

Transit Providers:

- **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.

	Customers	***Peers***	***Transits***
Type-1	0.3%	47%	99%
Type-4	0.0%	24%	99%
Realistic	0.0%	3%	99%
Omni			

Table: Reason why forged routes were visible

Realistic Hijackers

- **Easy to hide when exporting to Peer links.**
- **Hard to hide when exporting to transits.**

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.

	Customers	*Peers*	*Transits*
Type-1	0.3%	47%	99%
Type-4	0.0%	24%	99%
Realistic	0.0%	3%	99%
Omni	0%	0%	0%

Table: Reason why forged routes were visible

Realistic Hijackers

- **Easy to hide when exporting to Peer links.**
- **Hard to hide when exporting 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:

- ***Victim:*** Testbed site at *Wisconsin*.
- ***Hijacker:*** Testbed site at *GRNET* and *AMS-IX*.
- ***Goal:*** Design a stealthy hijack not observable by public RCs.

Real World Evaluation: PEERING Testbed

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

<u>Binary classification of monitors</u>

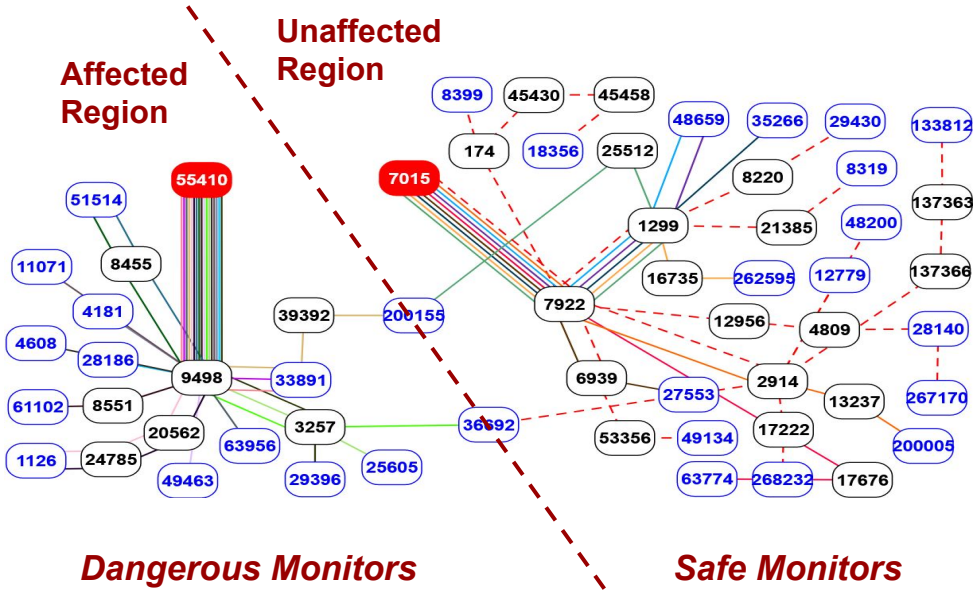
- ***Safe****:* Will **<u>not</u>** report the attack.
- ***Dangerous****:* Will report the attack.

Real World Evaluation: PEERING Testbed

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

<u>Binary classification of monitors</u>

- ***Safe****:* Will **<u>not</u>** report the attack.
- ***Dangerous****:* Will report the attack.

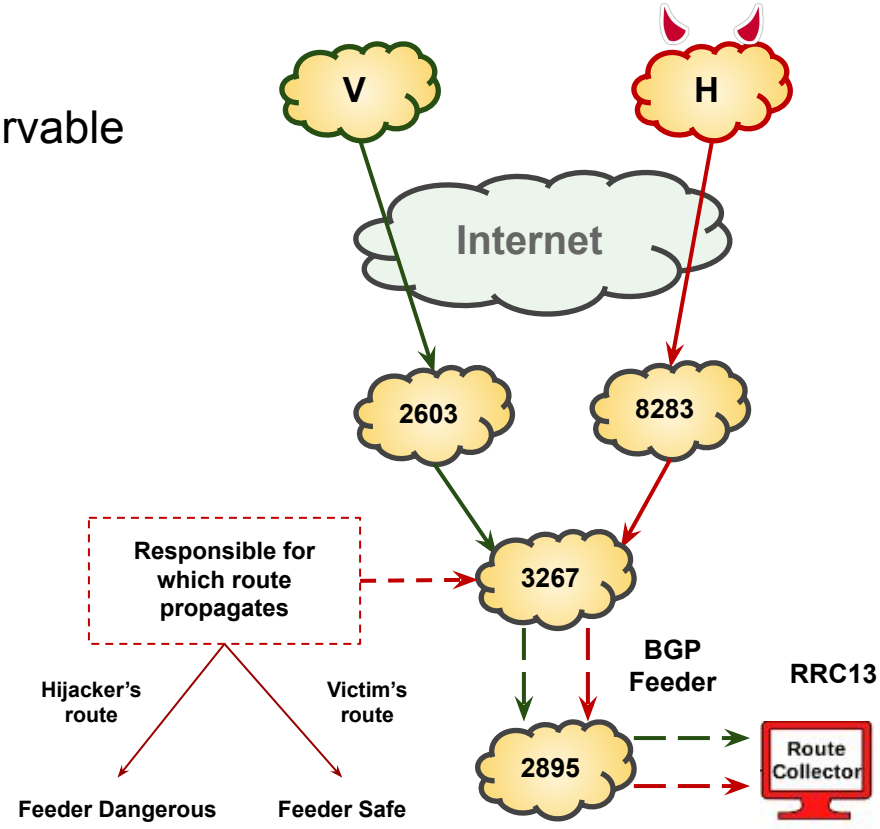


Real World Evaluation: PEERING Testbed

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

Binary classification of monitors

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



Real World Evaluation: PEERING Testbed

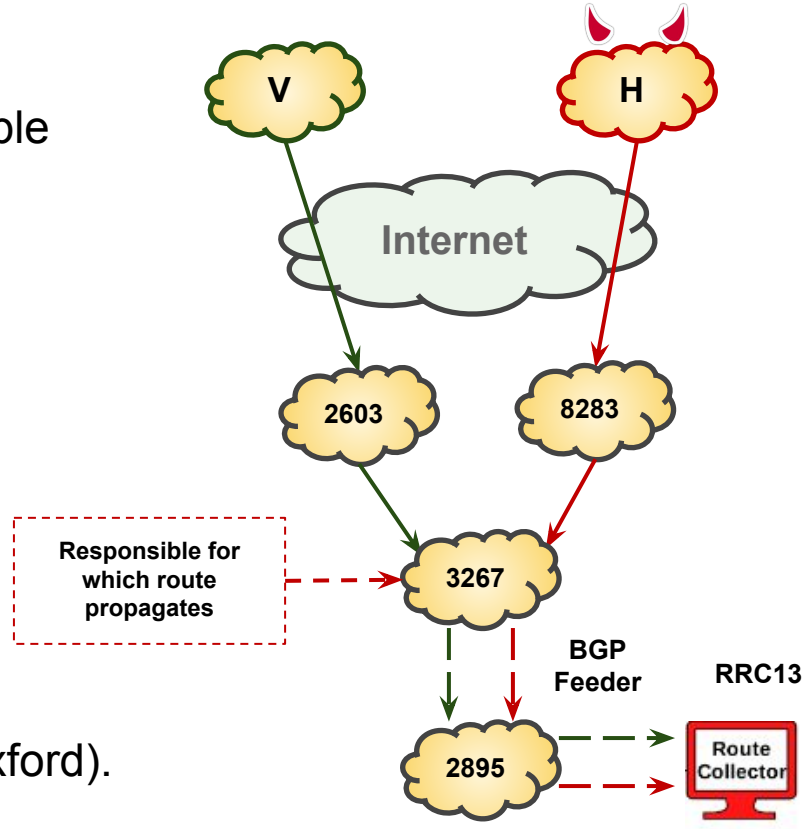
➔ ***Goal:*** Design a stealthy hijack not observable by public RCs.

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).



Statistics: 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*						
	Sensitivity (Specificity)						
% Monitors Correctly Classified Business Classifier	*Accuracy*						
	Sensitivity (Specificity)						

❖ ***Sensitivity (Specificity):*** % correctly classified *dangerous (safe)* monitors.

Statistics: 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*						
	Sensitivity (Specificity)						
% Monitors Correctly Classified Business Classifier	*Accuracy*						
	Sensitivity (Specificity)						

❖ ***Sensitivity (Specificity):*** % correctly classified *dangerous* *(safe)* monitors.

Statistics: 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%
	Sensitivity (Specificity)	13% *(99%)*	62% *(93%)*	75% *(91%)*	100% *(97%)*	**10%** *(94%)*	100% *(99%)*
% Monitors Correctly Classified Business Classifier	*Accuracy*						
	Sensitivity (Specificity)						

Transits: Average Accuracy = 78%

Proximity classifier not sufficient

(Overestimates Safe Monitors)

Peers: Possible to identify all dangerous monitors

Usually High specificity & sensitivity

(Outliers may exist)

❖ ***Sensitivity (Specificity):*** % correctly classified *dangerous (safe)* monitors.

Statistics: 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%
	Sensitivity (Specificity)	13% *(99%)*	62% *(93%)*	75% *(91%)*	100% *(97%)*	**10%** *(94%)*	100% *(99%)*
% Monitors Correctly Classified Business Classifier	*Accuracy*	90%	92%	89%	*Same*	*Same*	*Same*
	Sensitivity (Specificity)	95% *(89%)*	96% *(86%)*	97% *(81%)*	*Same*	*Same*	*Same*

Transits: Average Accuracy = 90%
reduces FNs (dangerous misclassifications) by <= 91%
Higher Sensitivity at the cost of Specificity

Peers: Practically unchanged

❖ ***Sensitivity (Specificity):*** % correctly classified *dangerous* *(safe)* monitors.

Conclusions

- RQ: How capable hijackers are to hide from Route Collectors (RCs)?
- What we learned:
  -
  -
  -
- Future Work:
  -
  -

Conclusions

- RQ: How capable hijackers are to hide from Route Collectors (RCs)?
- What we learned:
  - Traditional RCs may be vulnerable to stealthy attacks if the following properties hold:

    (1) Feeder reports their best routes to RC and **(2)** RC is Public.
  - Stealthy hijacks: may thrive in *Peer* links.
  - *Transit* links: Harder for hijackers to completely hide.
- Future Work:
  -
  -

Conclusions

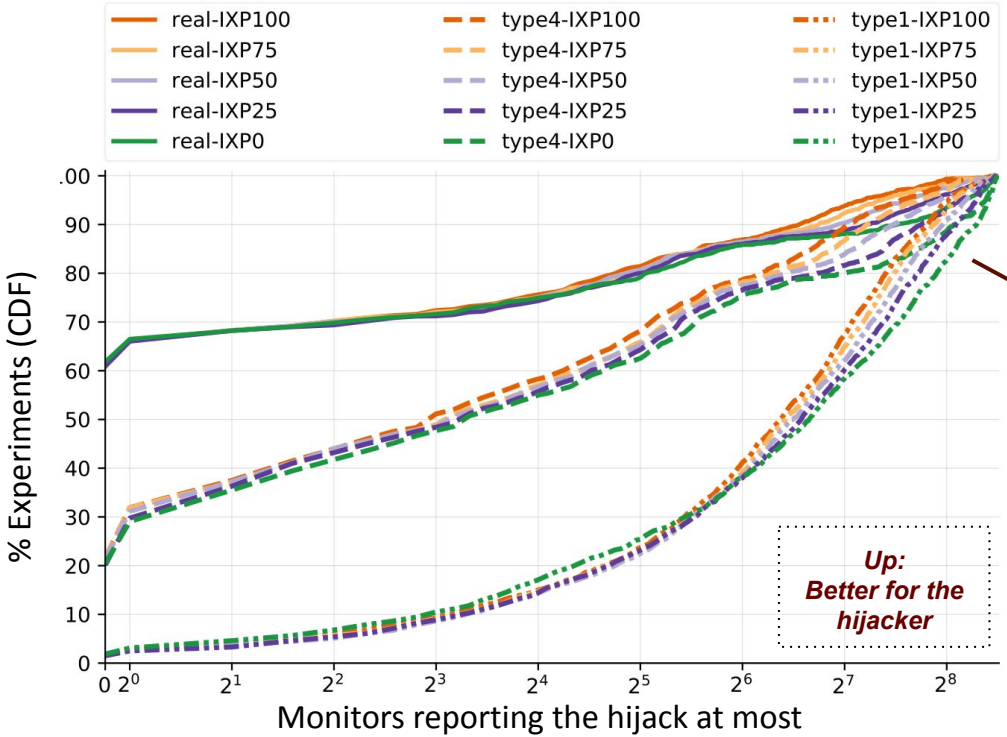
- RQ: How capable hijackers are to hide from Route Collectors (RCs)?
- What we learned:
  - Traditional RCs may be vulnerable to stealthy attacks if the following properties hold:

    (1) Feeder reports their best routes to RC and **(2)** RC is Public.
  - Stealthy hijacks: may thrive in *Peer* links.
  - *Transit* links: Harder for hijackers to completely hide.
- Future Work: Solutions against stealthy attacks.
  - Selecting new feeders in more strategic locations.
  - Benefits of BGP Monitoring Protocol (BMP).

thank you
danke
рахмат
謝謝
ngiyabonga
teşekkür ederim
Баярлалаа
спасибо
mersi
kia ora
barka
welalin
tack
spas
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
mahalo
tapadh leat
gracias
kiitos
dankie
nanni
nandri
dhanyavad
mauruuru
köszönöm
hvala
gràcie
bayarlalaa
bedankt
enkosi
dziękuję
aciu
dankon
akun
хвала
asante
manana
obrigada
tenki
djiere dieuf
tau
mochchakkeram
murakoze
дякую
mamnun
chokrane
chnorakaloutioun
grafias ago
gràcies
sulpáy
go raibh maith agat
sobodi
dėkuji
sagolun
sukriya
kop khun krap
taiku
obrigado
mèsi
ありがとう
tanemirt
grazie
arigatô
takk
dakujem
trugarez
najis tuke
didi madloba
kam sah hamnida
rahmat
terima kasih
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
merce
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci

Appendix

Appendix – Topologies With More IXP Links



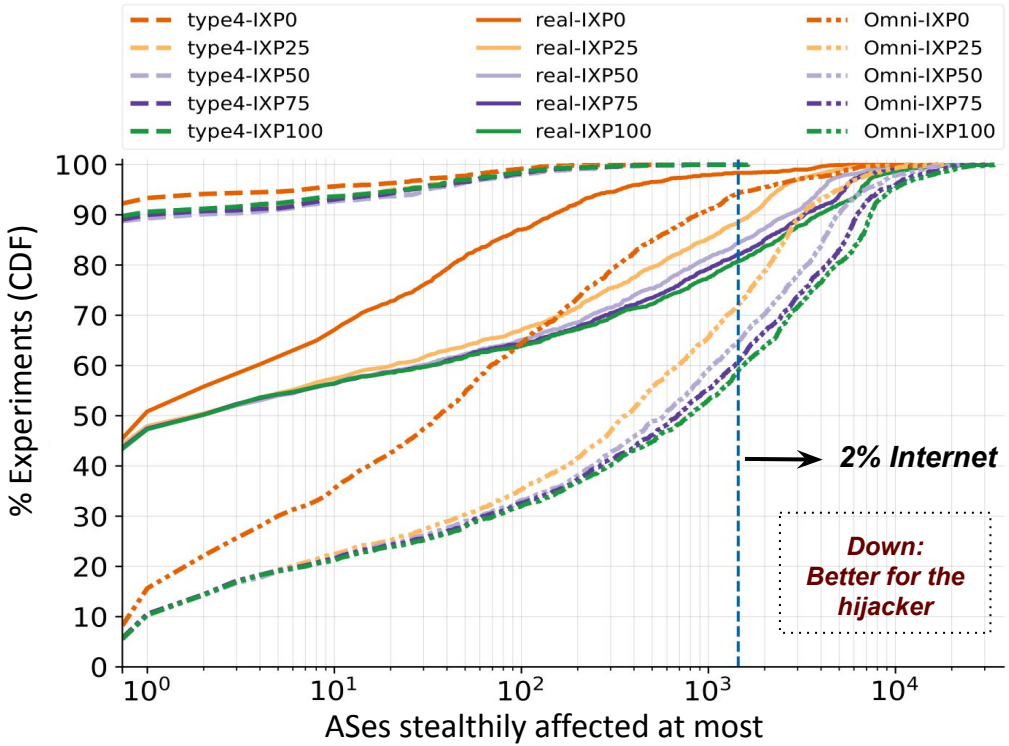
Adding more IXP links

- 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

Appendix – Topologies With More IXP Links



Adding more IXP links

- Stealthy hijacks more impactful

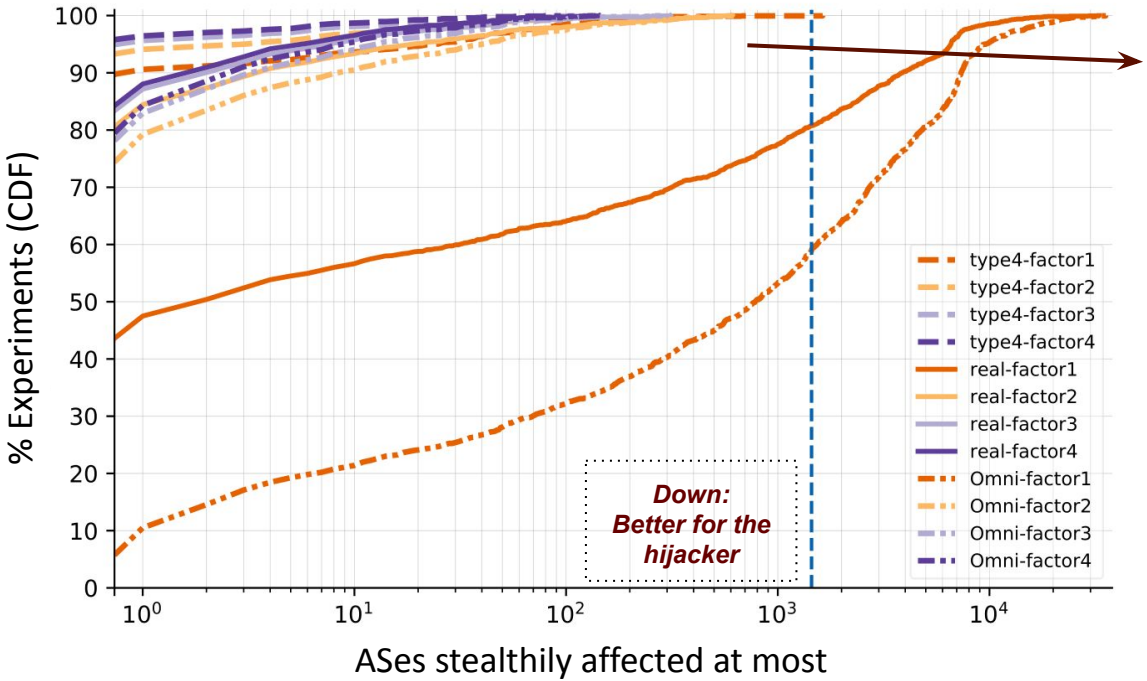
Traditional Topology (IXP0)

- 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

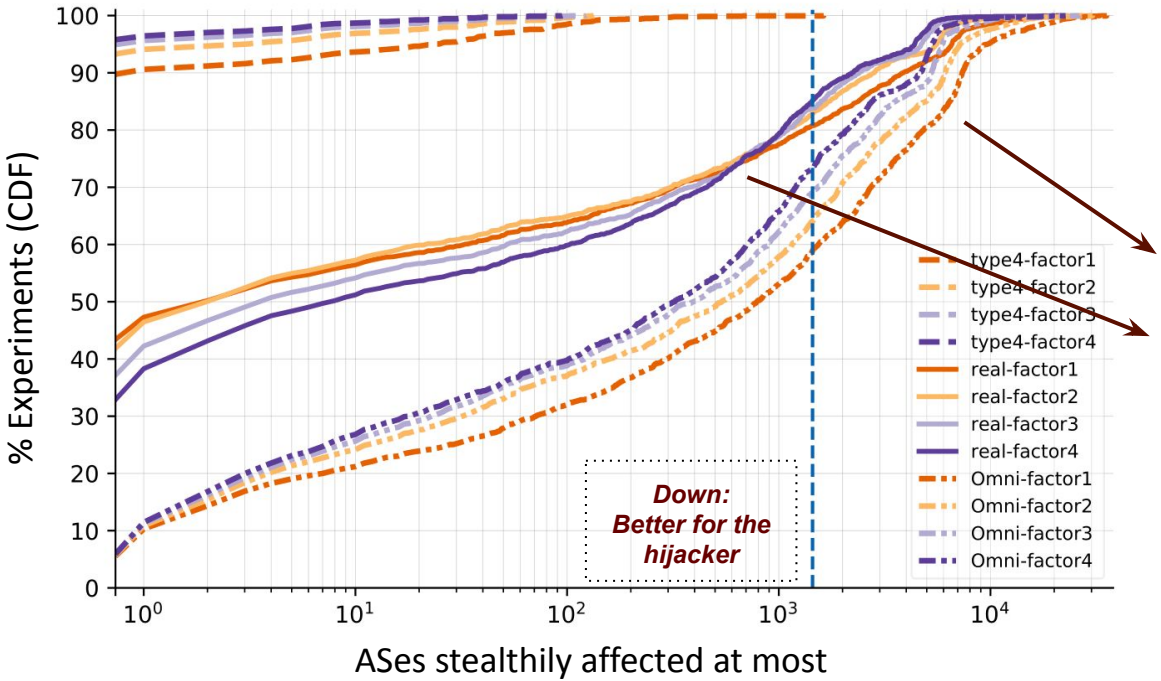
Appendix – Topologies With More Monitors



Non-Reactive Hijackers

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

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

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**