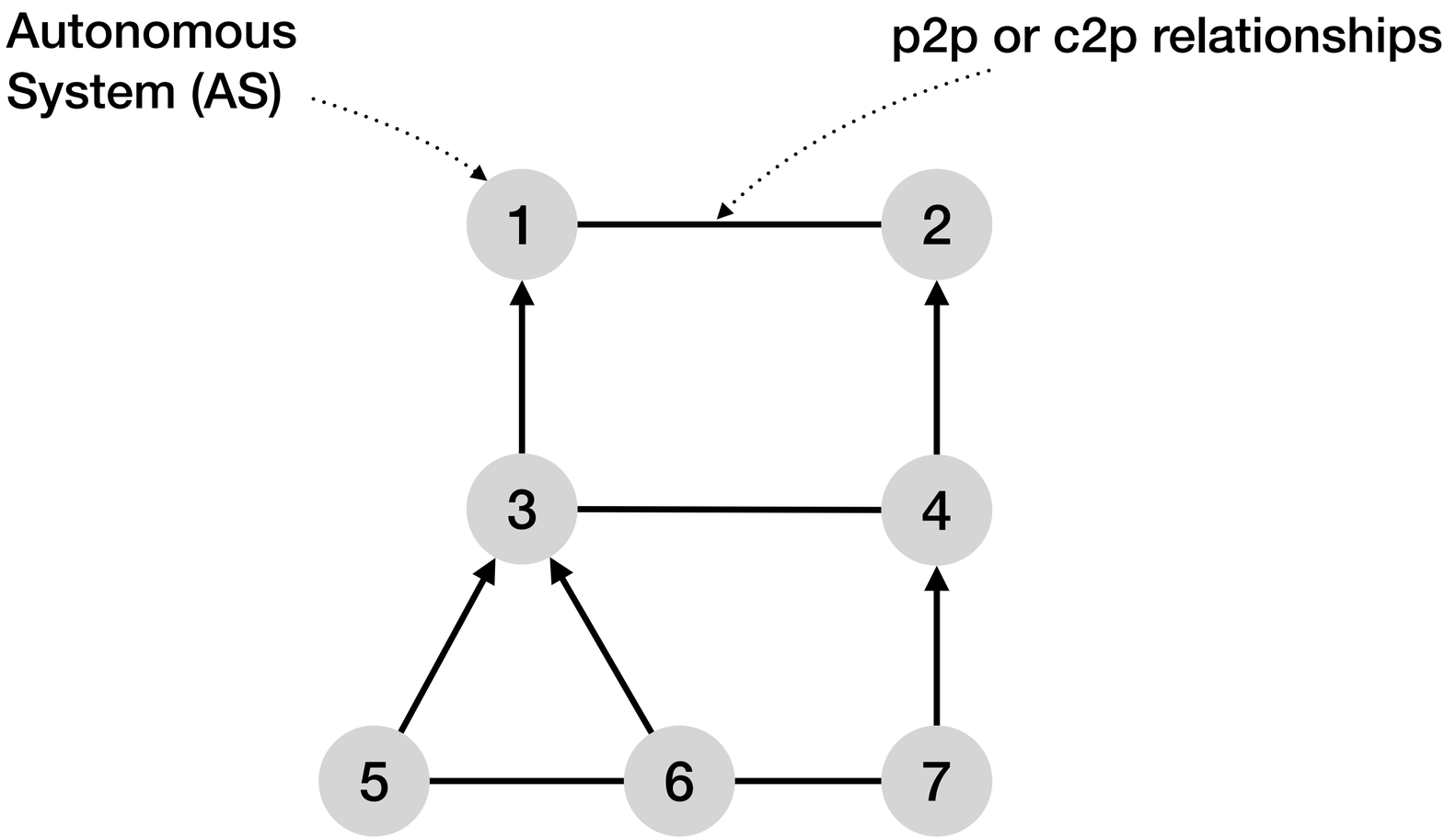
A System to Detect Forged-Origin Hijacks

https://dfoh.uclouvain.be

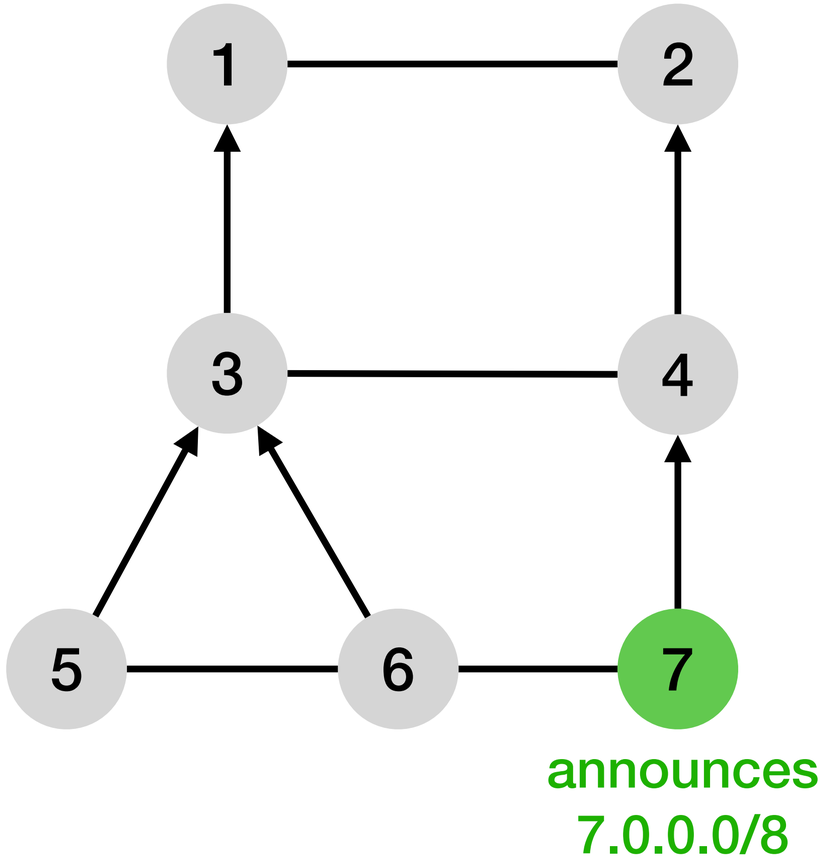
Thomas Holterbach
MANRS Ambassador 2023
University of Strasbourg

Joint work with:
Thomas Alfroy
Amreesh D. Phokeer
Alberto Dainotti
Cristel Pelsser

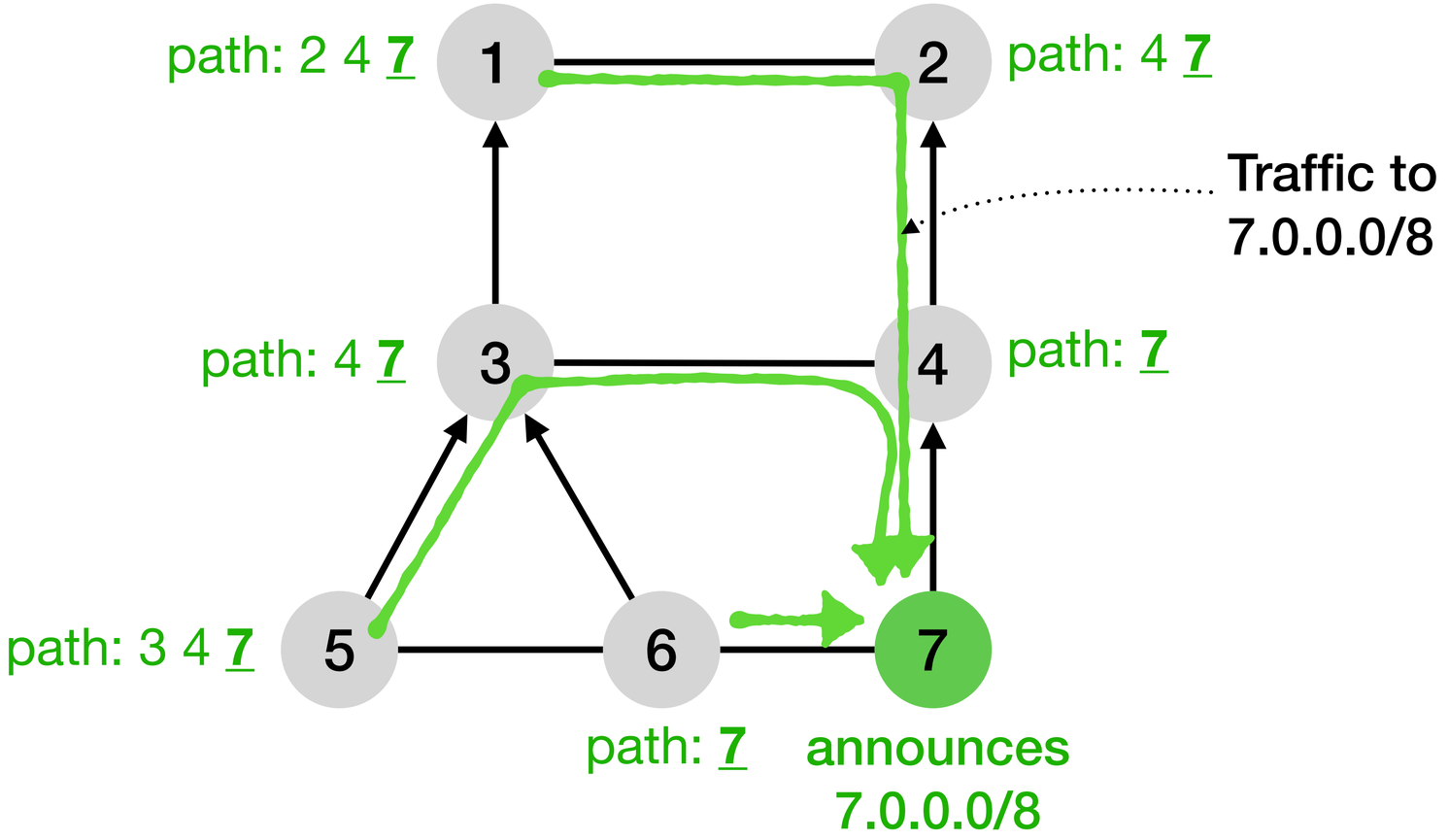
Internet routing (BGP) is vulnerable to traffic hijacking



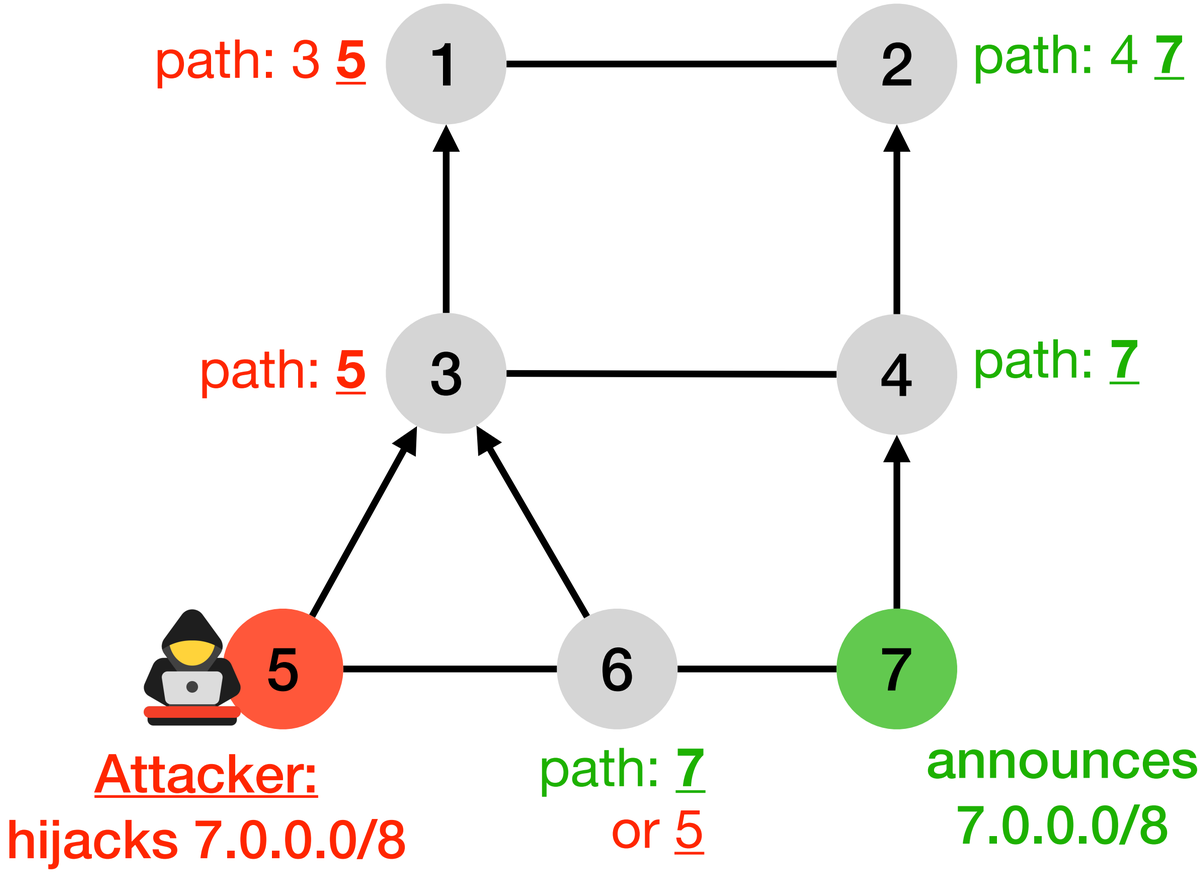
Internet routing (BGP) is vulnerable to traffic hijacking



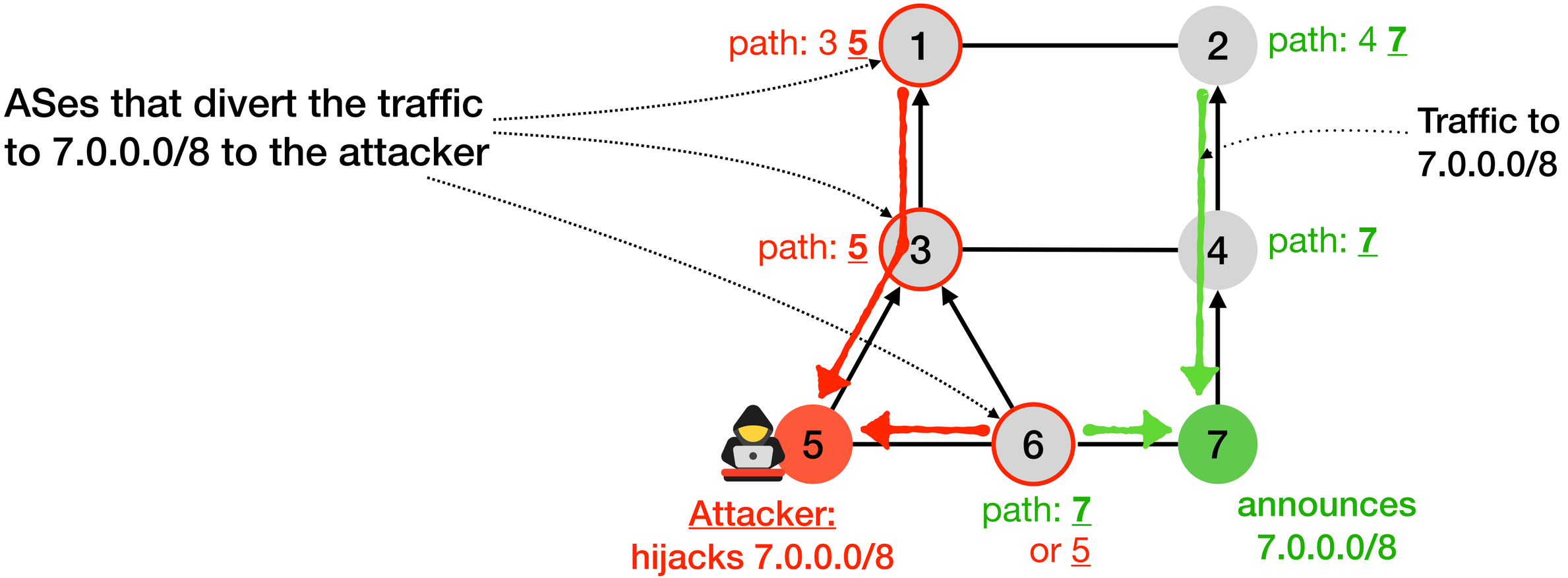
Internet routing (BGP) is vulnerable to traffic hijacking



Internet routing (BGP) is vulnerable to traffic hijacking



Internet routing (BGP) is vulnerable to traffic hijacking

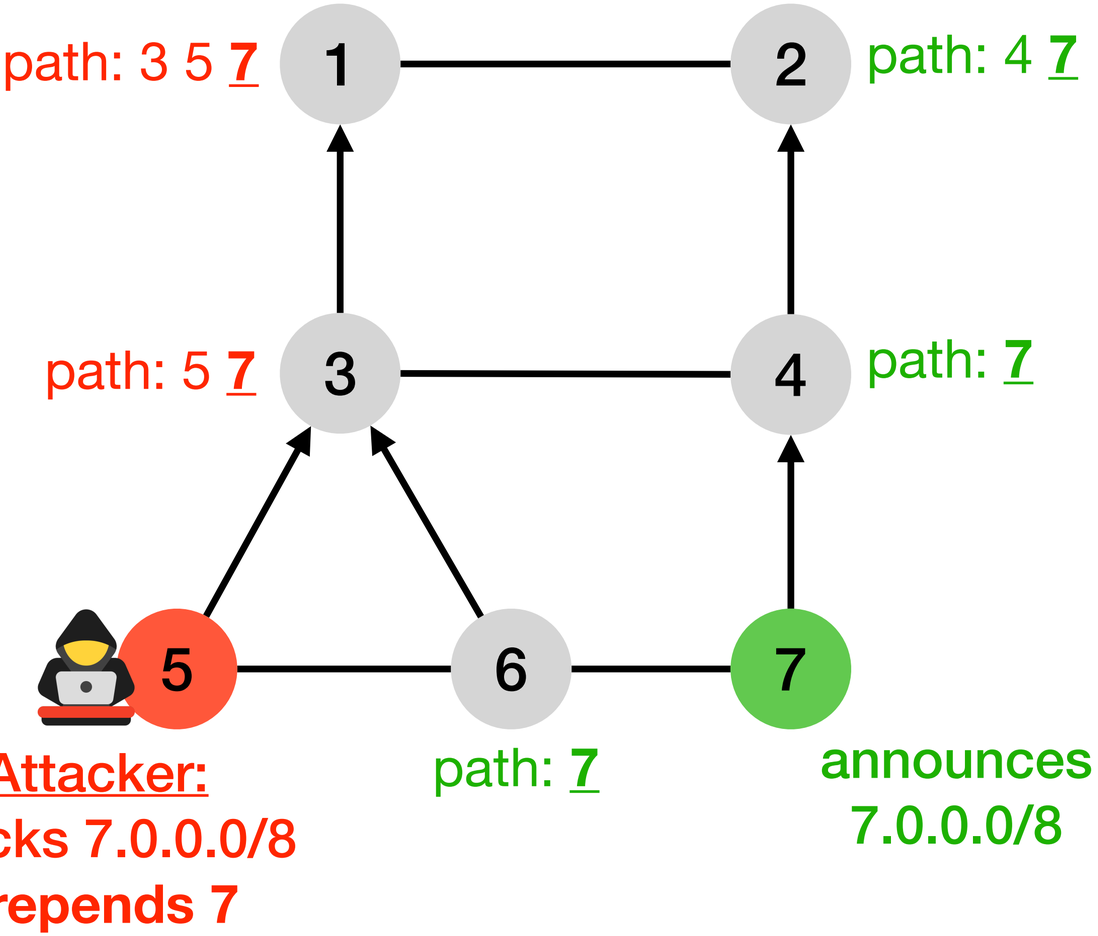


Fortunately, there are defenses against BGP hijacking

Protocol extensions	RPKI + ROV BGPSec, ASPA
Configuration guidelines	Route filters
Monitoring platforms	ARTEMIS BGPAlerter

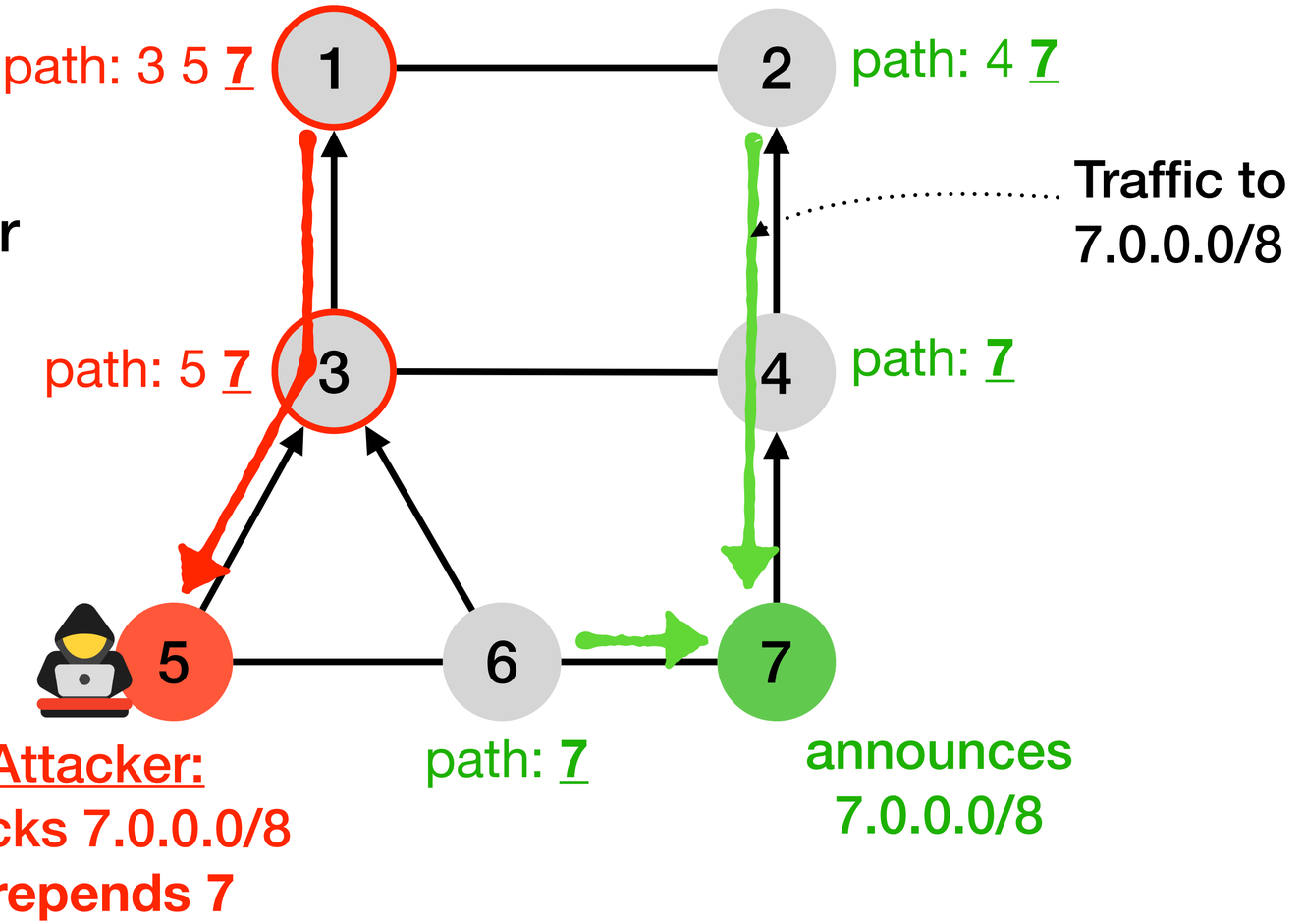
Despite the efforts, BGP is *still* vulnerable to forged-origin hijacks

The attacker prepends the legitimate AS number to the AS path



Despite the efforts, BGP is *still* vulnerable to forged-origin hijacks

Less but still a significant fraction of the traffic is diverted to the attacker



Existing defenses poorly neutralise forged-origin hijacks

Protocol extensions	RPKI + ROV BGPSec, ASPA	RPKI+ROV can't detect forged-origin hijacks BGPSec and ASPA will take years to be widely deployed
Configuration guidelines	Route filters	Often missing and inaccurate as they are constructed based on the IRR
Monitoring platforms	ARTEMIS BGPAlerter	Narrowly focused as they detect hijacks that only pertain to the AS deploying it

Forged-origin hijacks are actively used by attackers

The Record.
Recorded Future® News

February 3, 2022

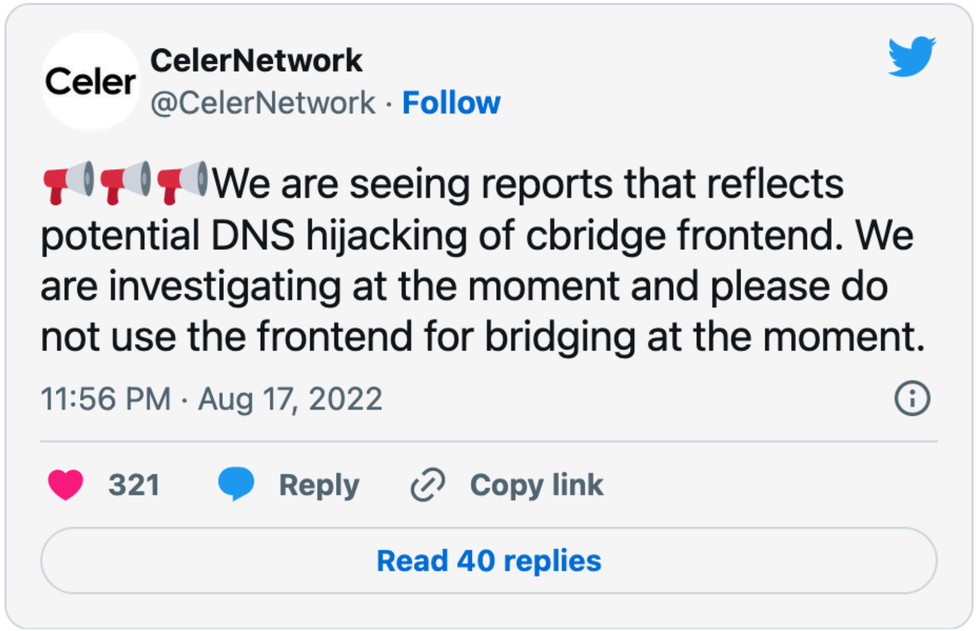
KlaySwap crypto users lose funds after BGP hijack

Hackers have stolen roughly $1.9 million from South Korean cryptocurrency platform KLAYswap after they pulled off a rare and clever BGP hijack against the server infrastructure of one of the platform's providers.

The BGP hijack—which is the equivalent of hackers hijacking internet routes to bring users on malicious sites instead of legitimate ones—hit KakaoTalk, an instant messaging platform popular in South Korea.

The attack took place earlier this month, on February 3, lasted only for two hours, and KLAYswap has confirmed the incident last week and is currently issuing compensation for affected users.

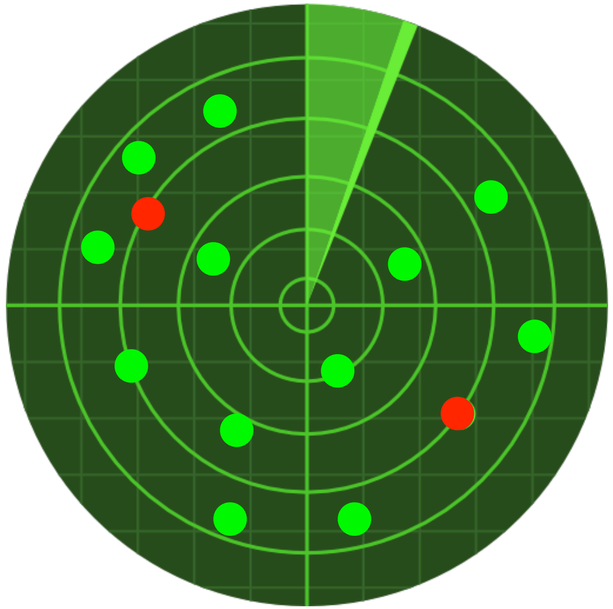
August 17, 2022



Both attacks are the result of a forged-origin hijack

DFOH: A System to Detect Forged-Origin Hijacks on the Whole Internet

Thomas Holterbach
University of Strasbourg



Joint work with:
Thomas Alfroy
Amreesh D. Phokeer
Alberto Dainotti
Cristel Pelsser

Outline

DFOH's main challenge

DFOH's inference pipeline

DFOH's inferences are accurate

***DFOH** is* up and running

Outline

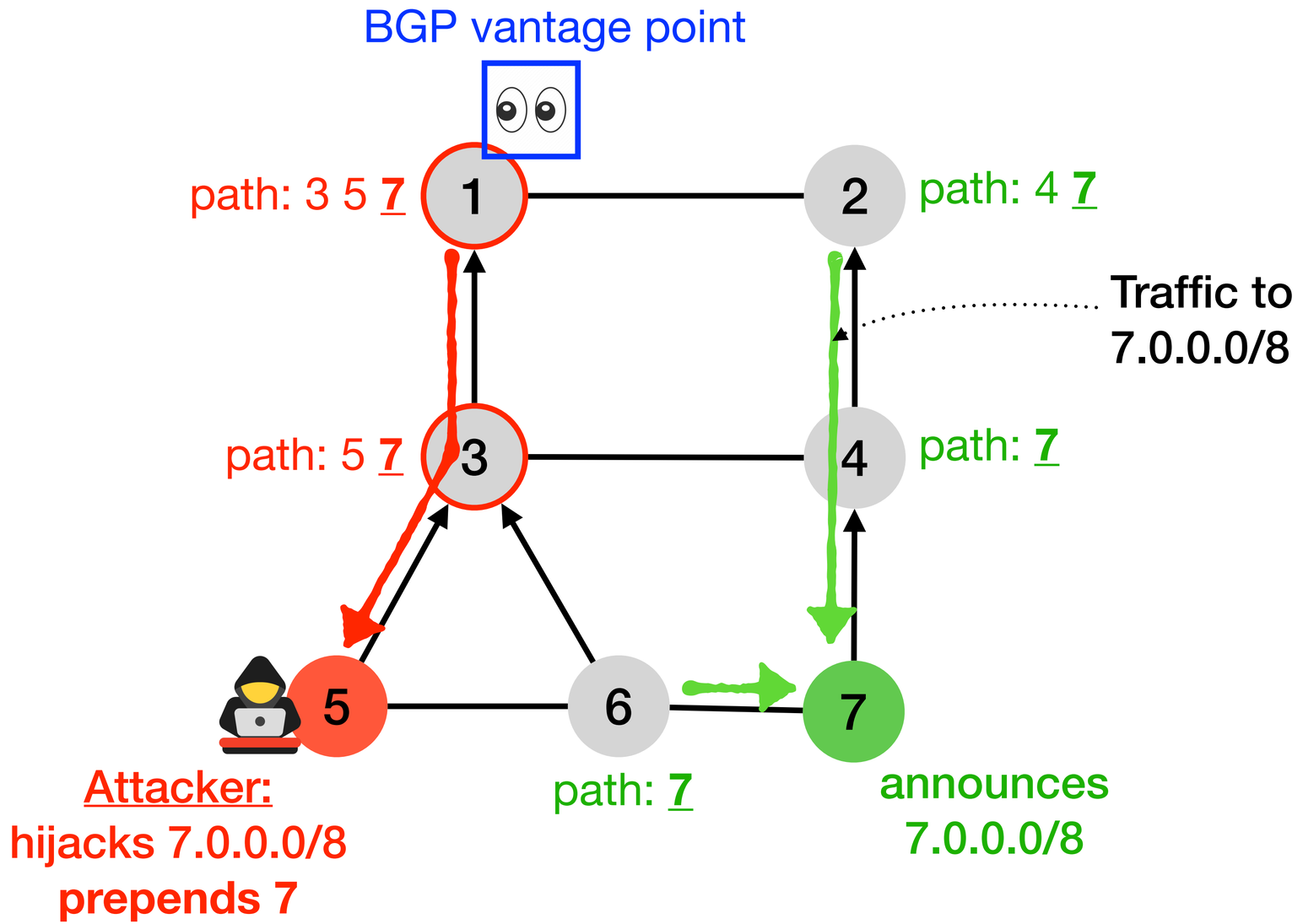
DFOH's main challenge is to detect fake AS links

DFOH's inference pipeline

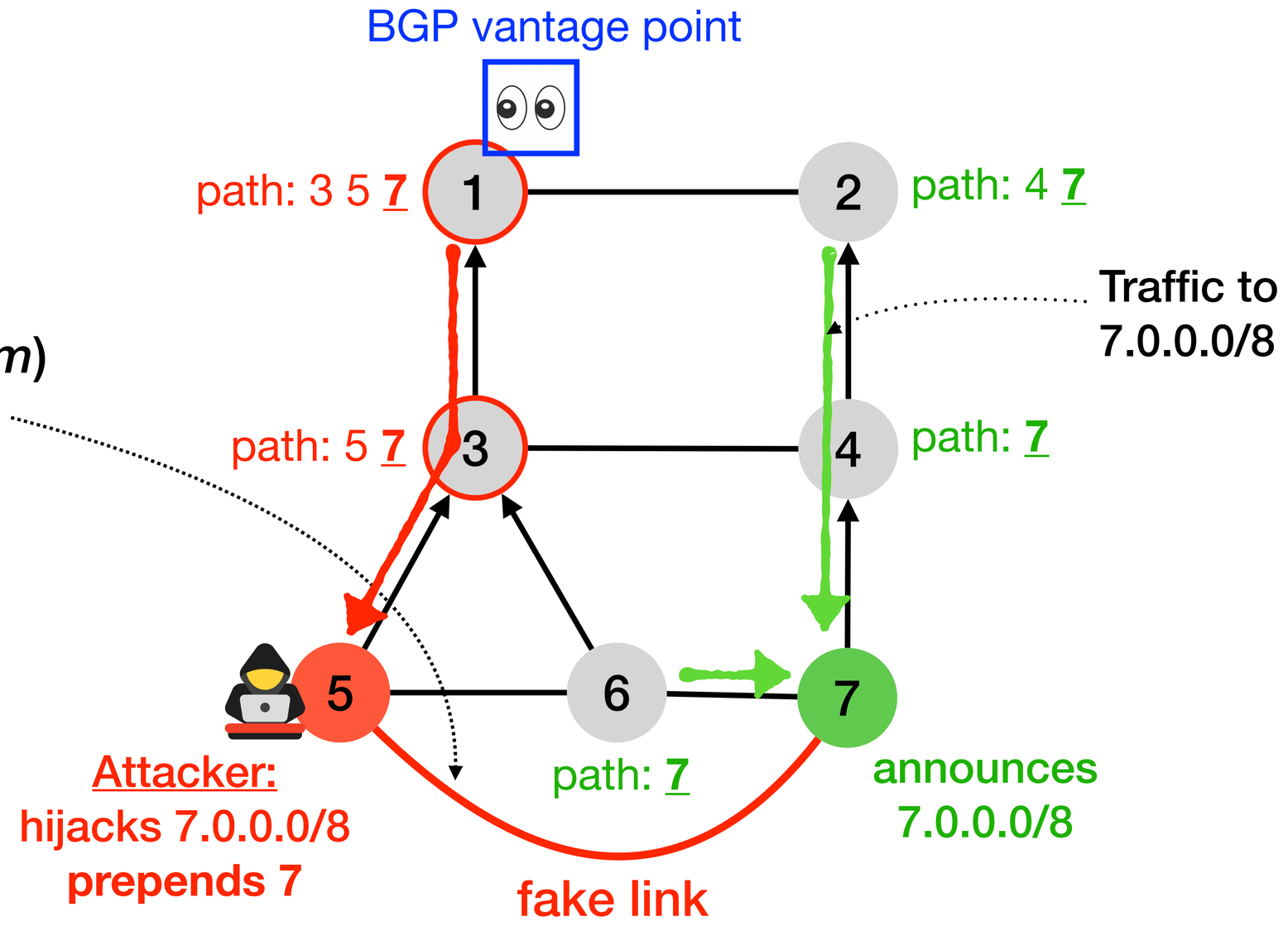
DFOH's inferences are accurate

***DFOH** is* up and running

DFOH aims to detect the fake AS links induced by forged-origin hijacks



DFOH aims to detect the fake AS links induced by forged-origin hijacks

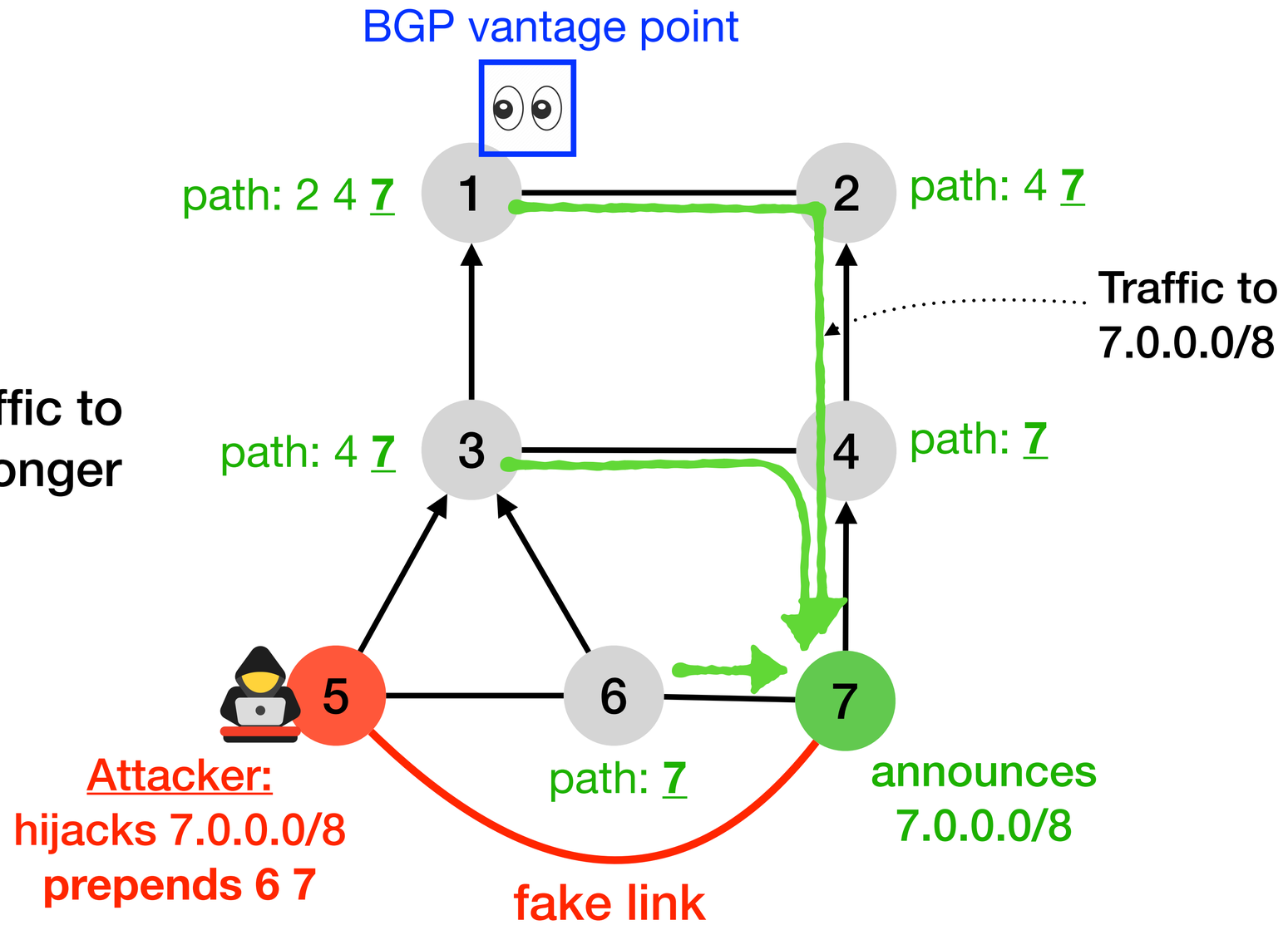


Upon the attack:
AS5 (*attacker*) and AS7 (*victim*) appear directly connected

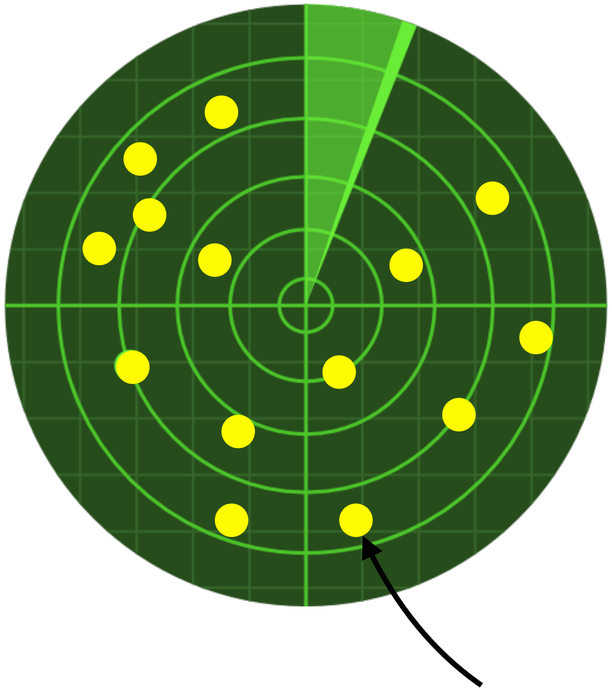
An attacker cannot escape from creating a new AS link without hampering the effectiveness of its attack

There is no new AS link if the attacker prepends **6 7**

But none of the ASes divert traffic to the attacker as the AS path is longer



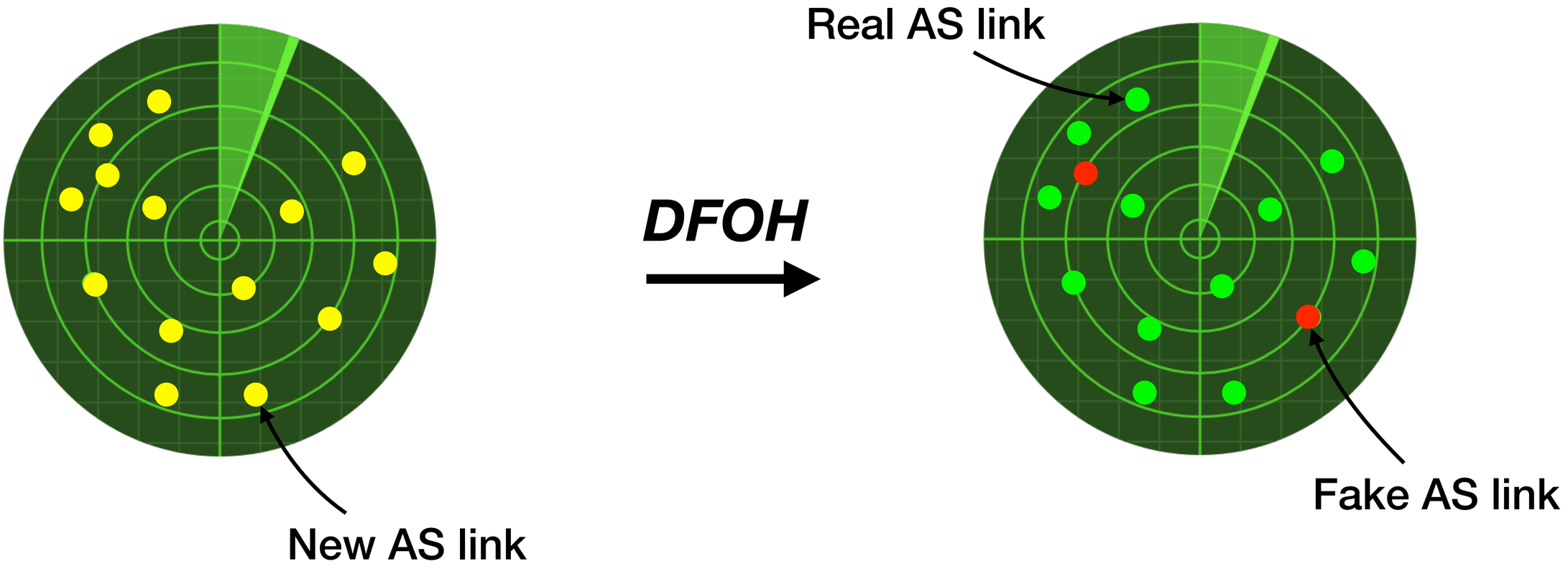
<u>Problem:</u> There are many new AS links every day
but no simple property that tells whether they are real or fake



We find 166 new AS links
every day (median)

Using the BGP data from 200 RIS and RouteViews
peers and collected during ten months in 2022

<u>Problem:</u> There are many new AS links every day
but no simple property that tells whether they are real or fake



Outline

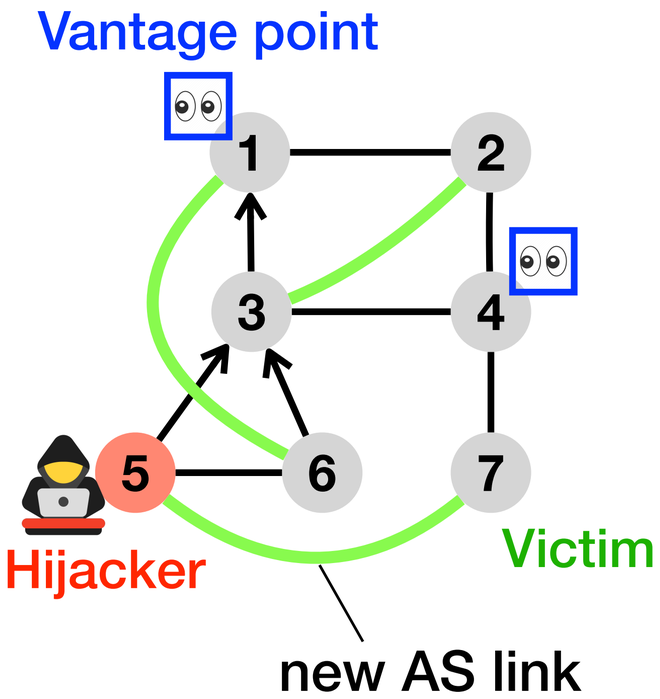
DFOH's main challenge — is to detect fake AS links

DFOH's inference pipeline — discriminates fake AS links from the real ones

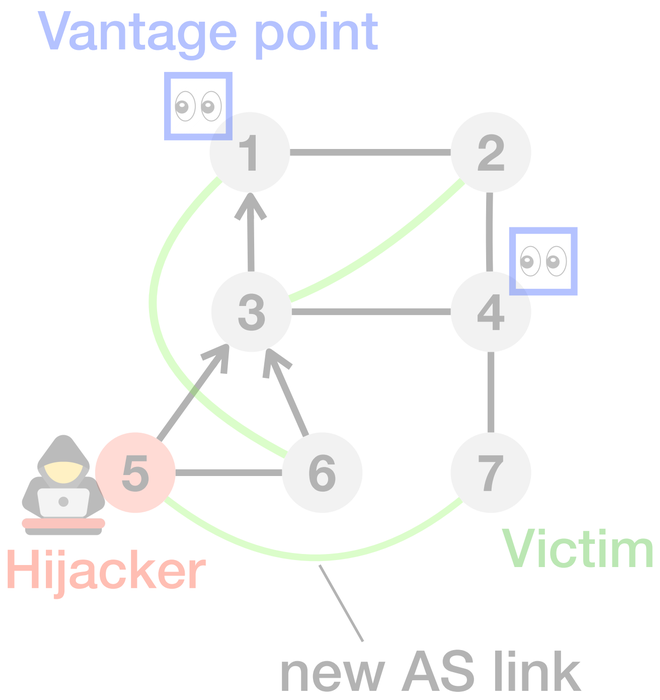
DFOH's inferences are accurate

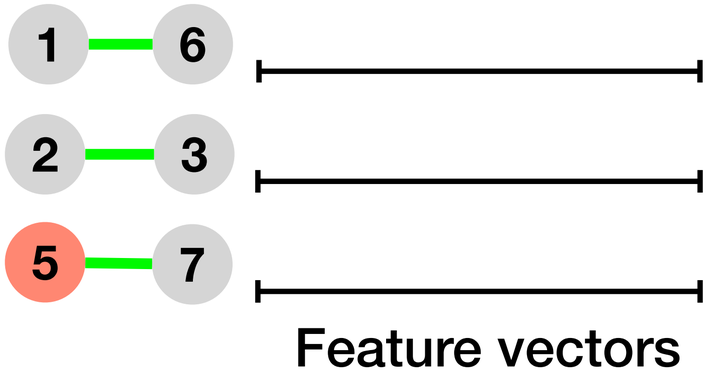
DFOH is up and running

DFOH's fake AS links inference algorithm comprises three steps

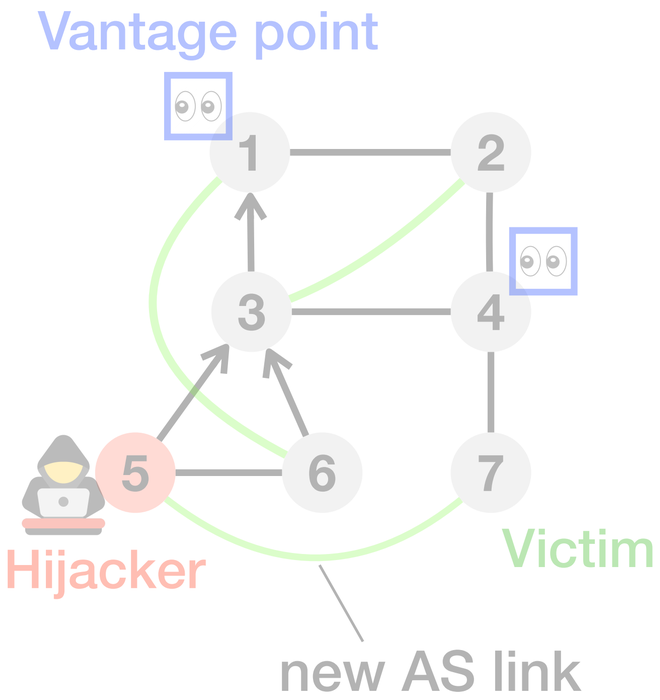


DFOH's fake AS links inference algorithm comprises three steps

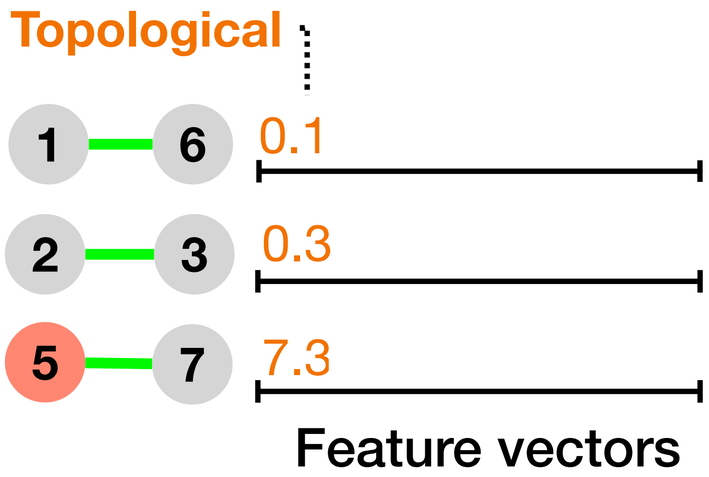




DFOH's fake AS links inference algorithm comprises three steps

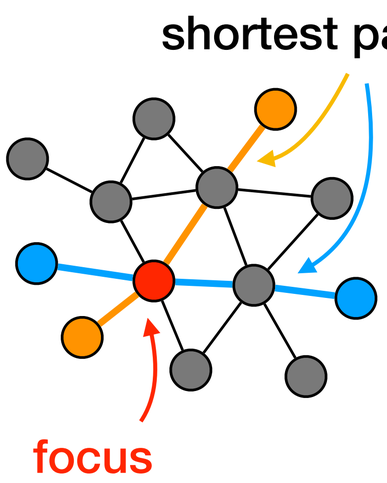


Feature categories:

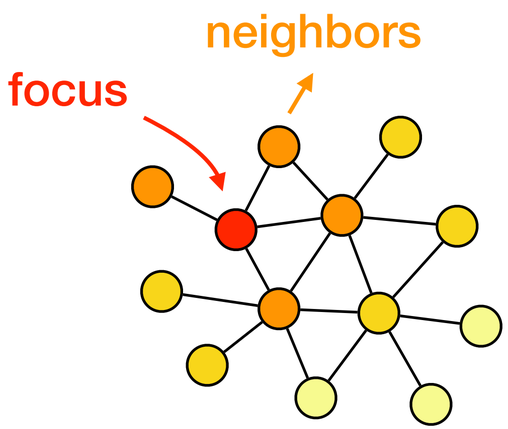


DFOH uses a total of 11 topological features that can be divided into four categories

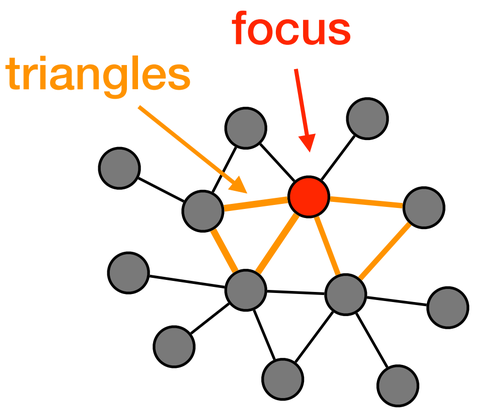
Node centrality



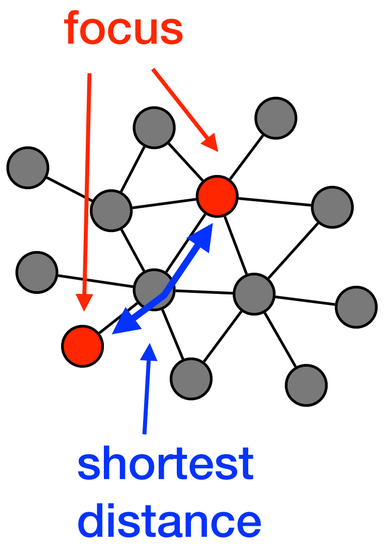
Neighborhood richness



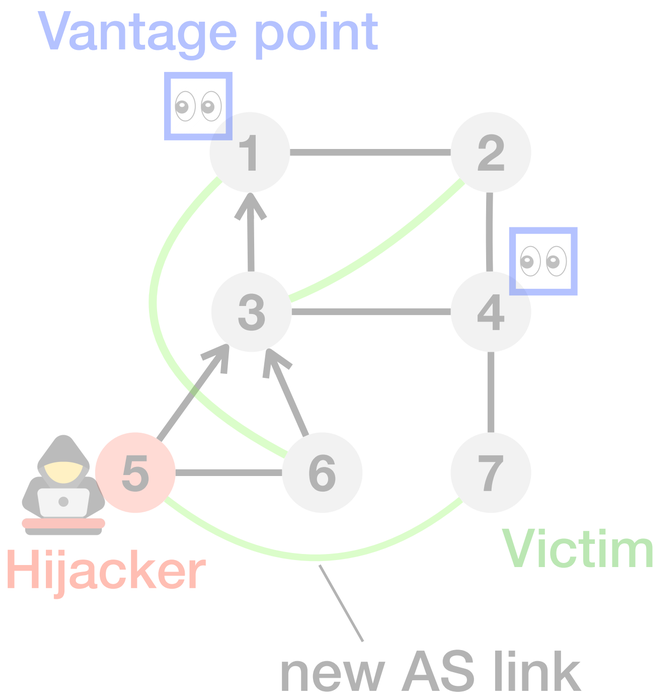
Topological patterns



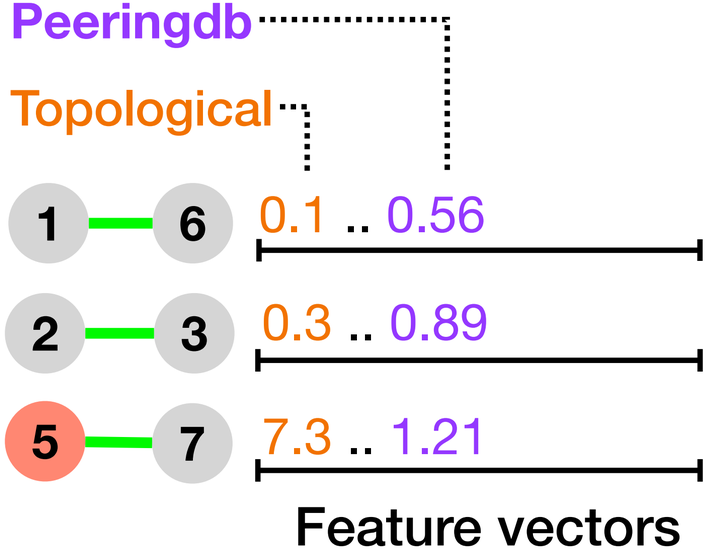
Closeness



DFOH's fake AS links inference algorithm comprises three steps



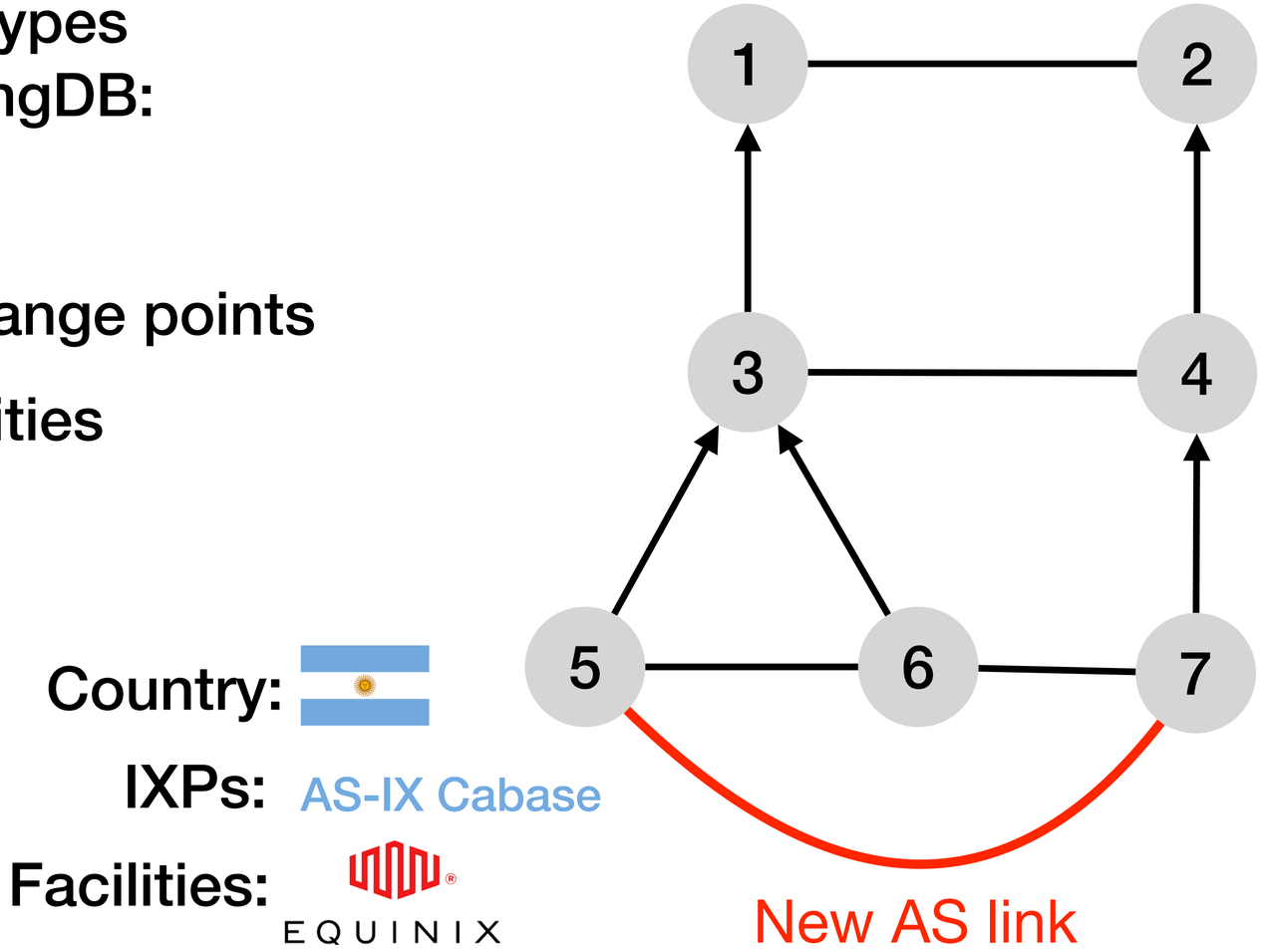
Feature categories:



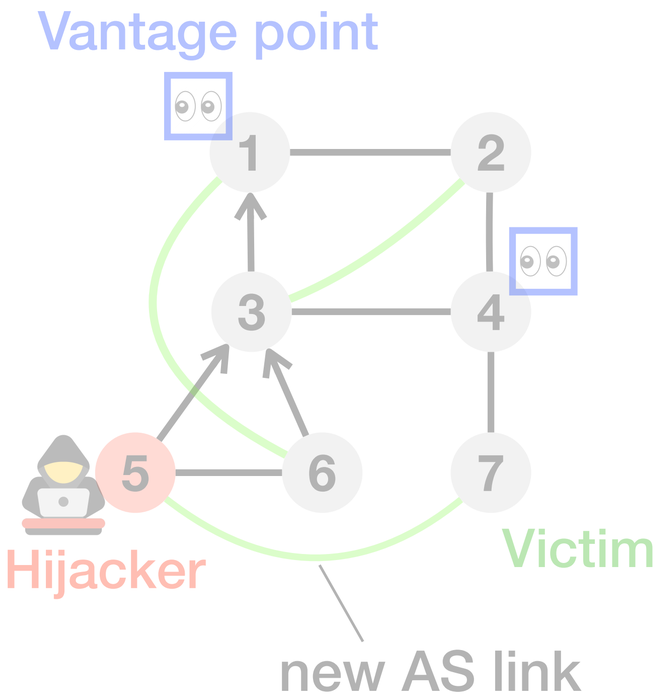
DFOH leverages correlations in the public peering information

DFOH looks for three types of information in PeeringDB:

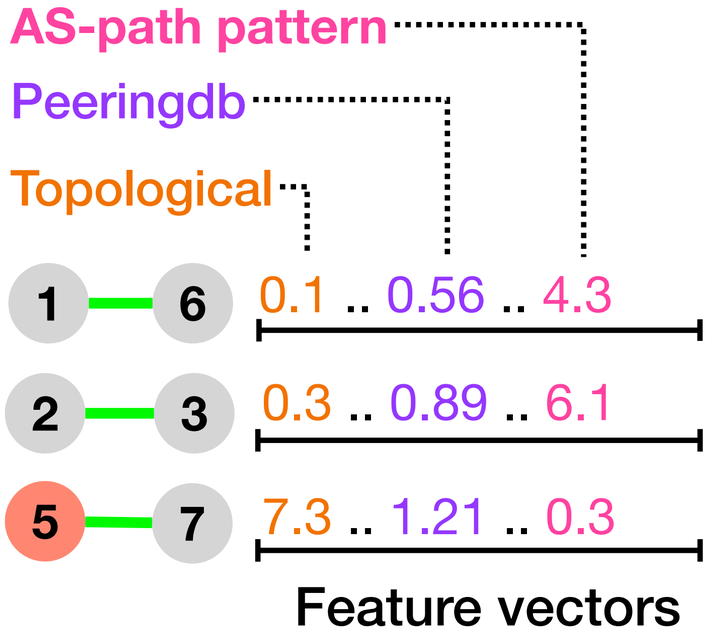
1. Country
2. Public peering exchange points
3. Private peering facilities



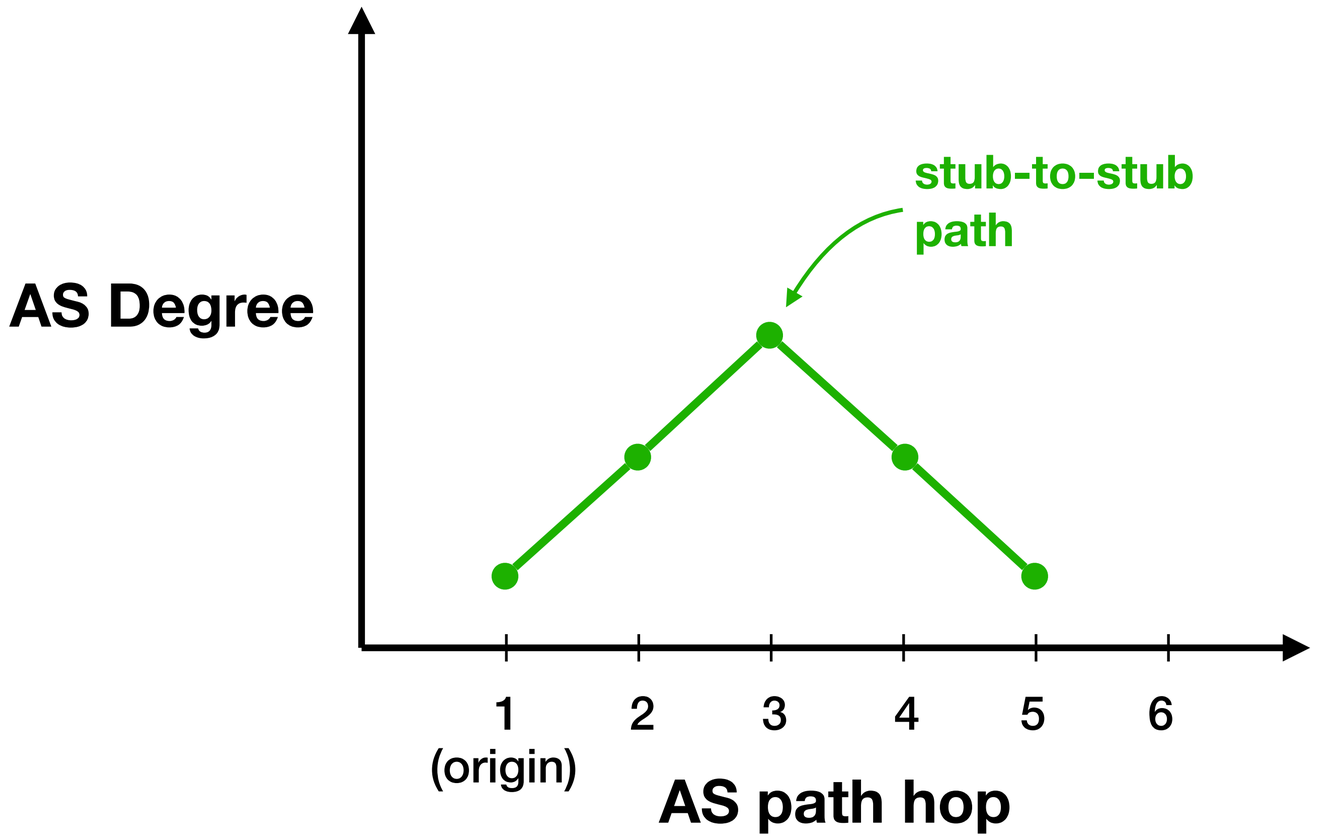
DFOH's fake AS links inference algorithm comprises three steps



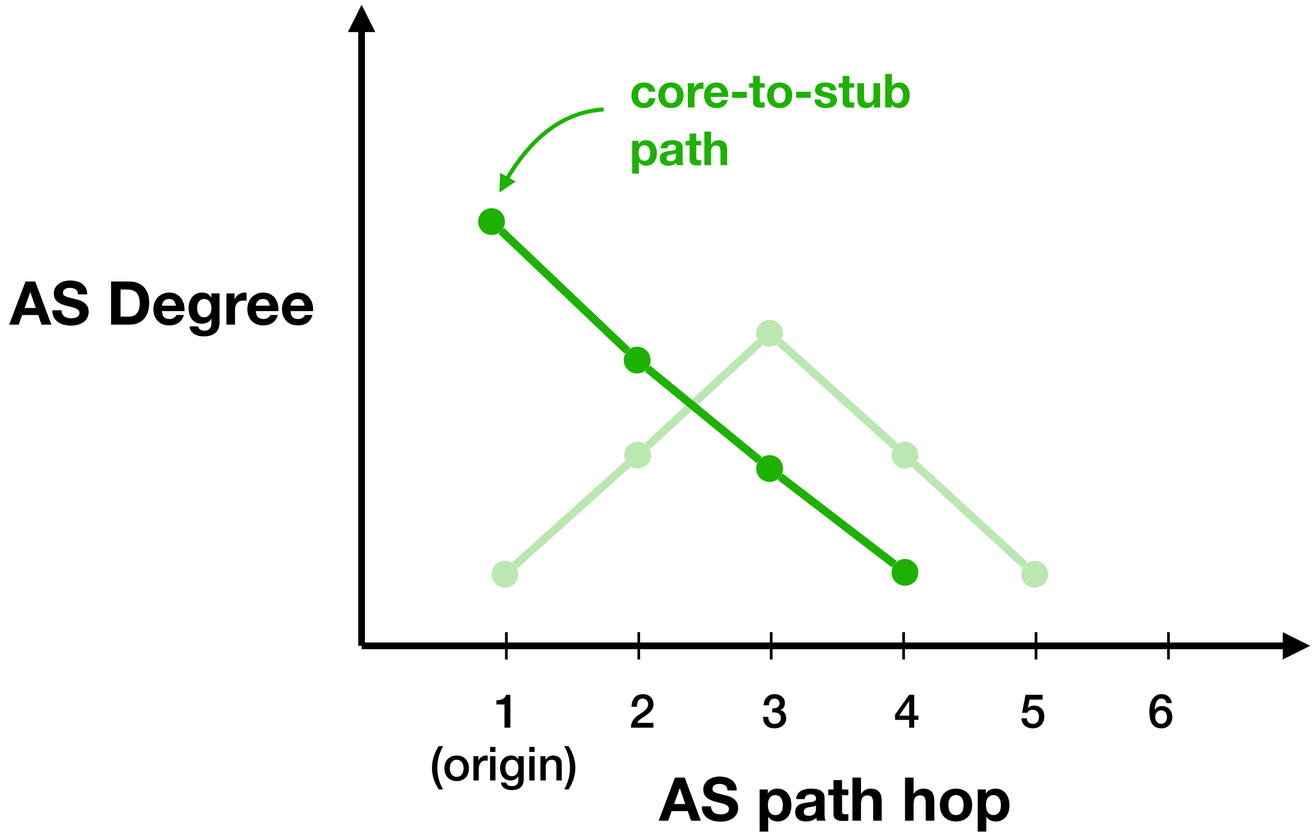
Feature categories:



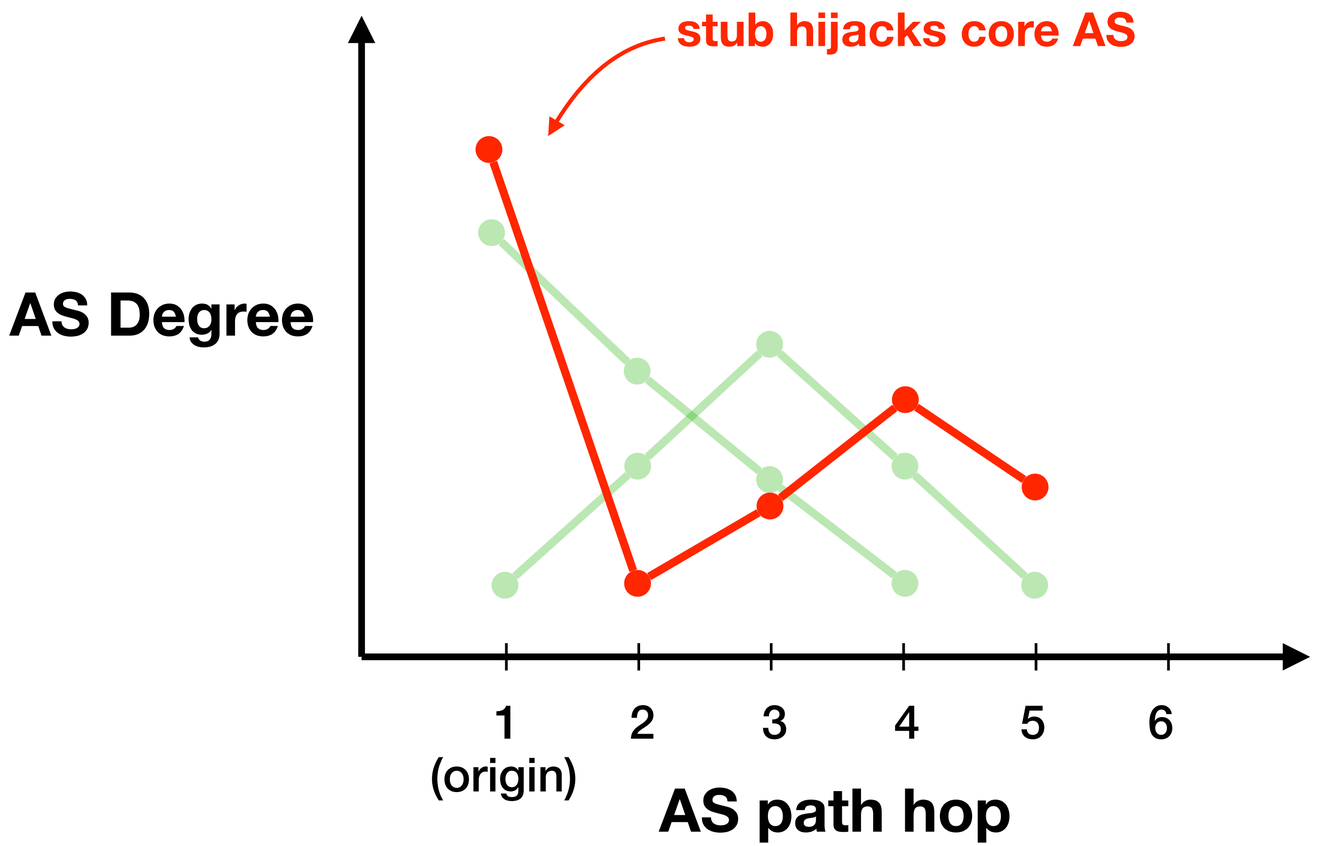
DFOH **detects fake AS paths as they often violate patterns induced by business relationships**



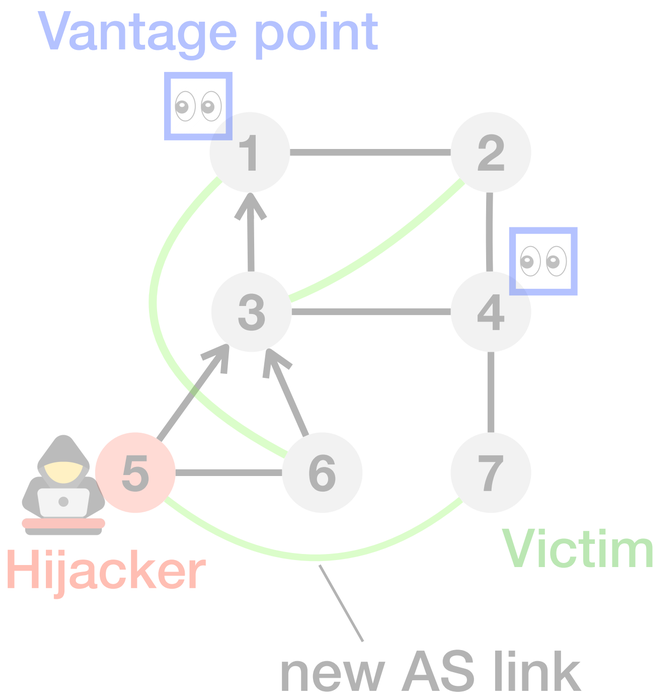
DFOH **detects fake AS paths as they often violate patterns induced by business relationships**

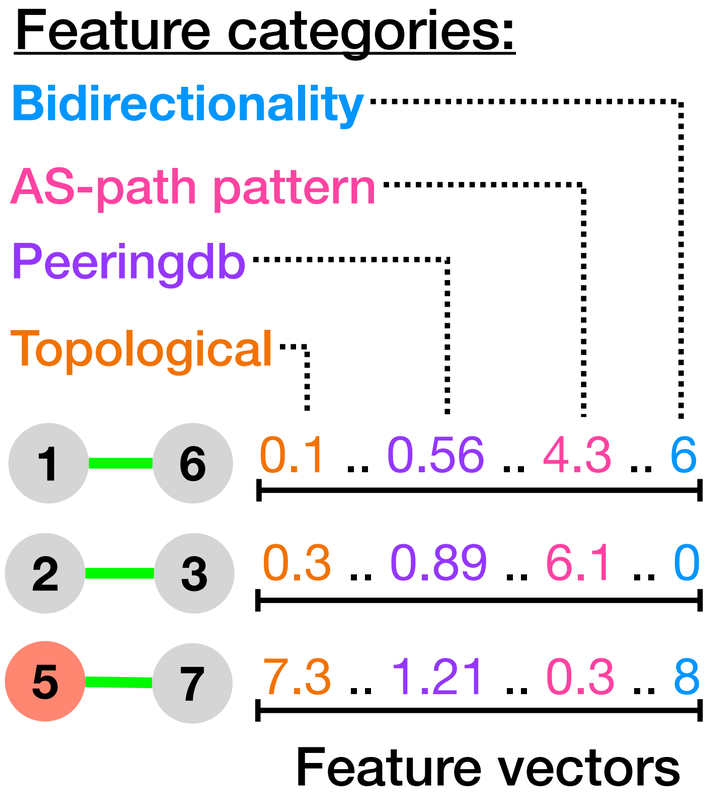


DFOH detects fake AS paths as they often violate patterns induced by business relationships

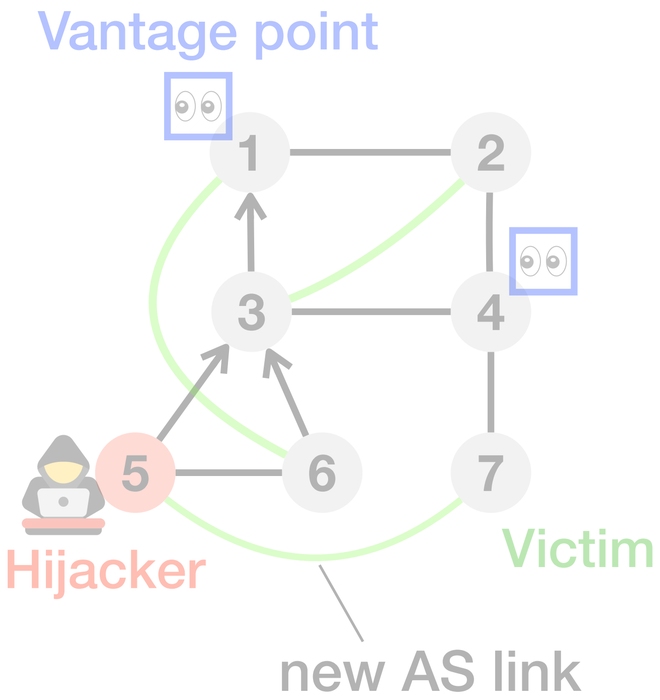


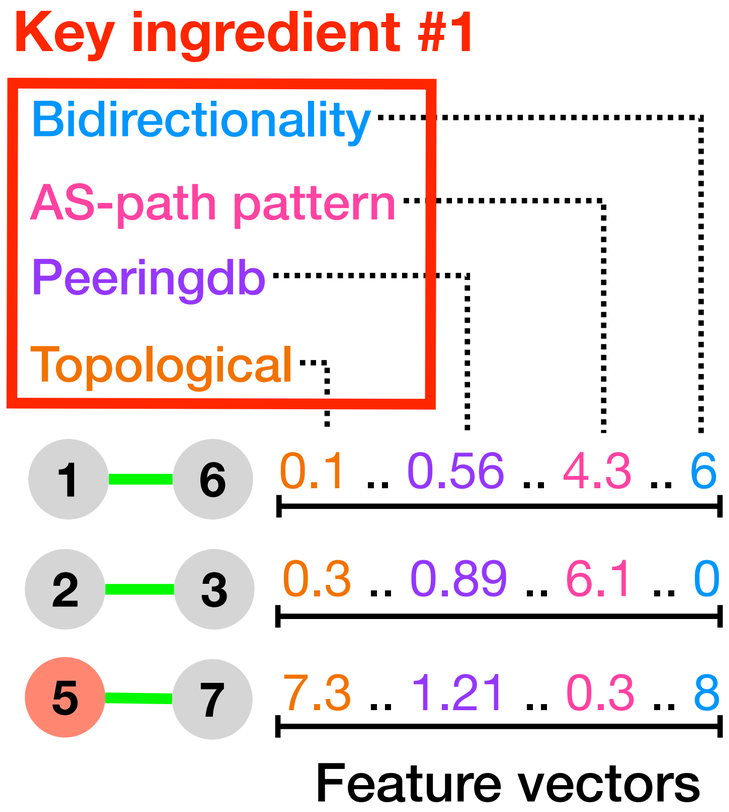
DFOH's fake AS links inference algorithm comprises three steps



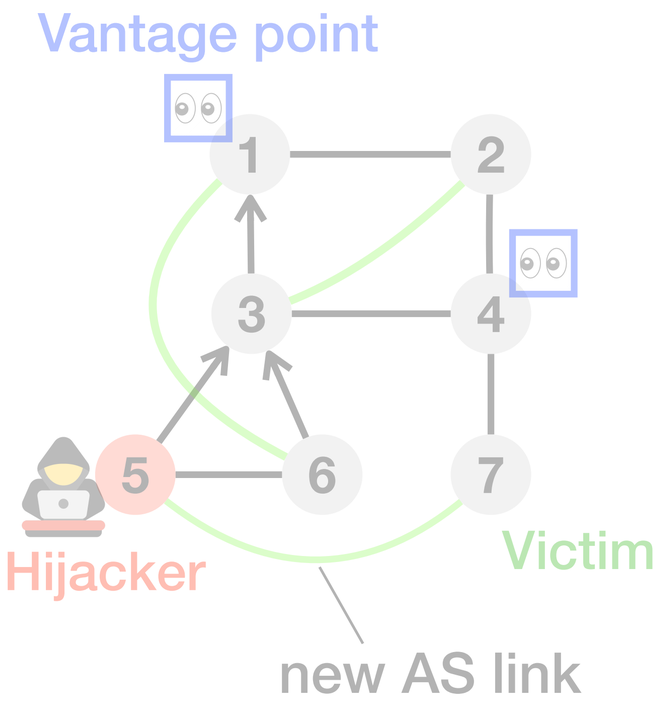


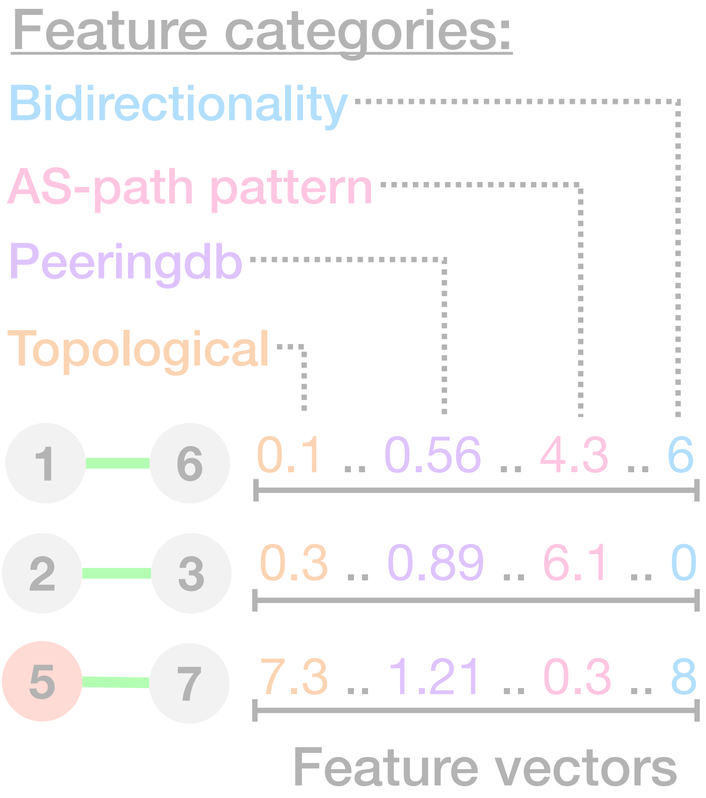
DFOH's fake AS links inference algorithm comprises three steps

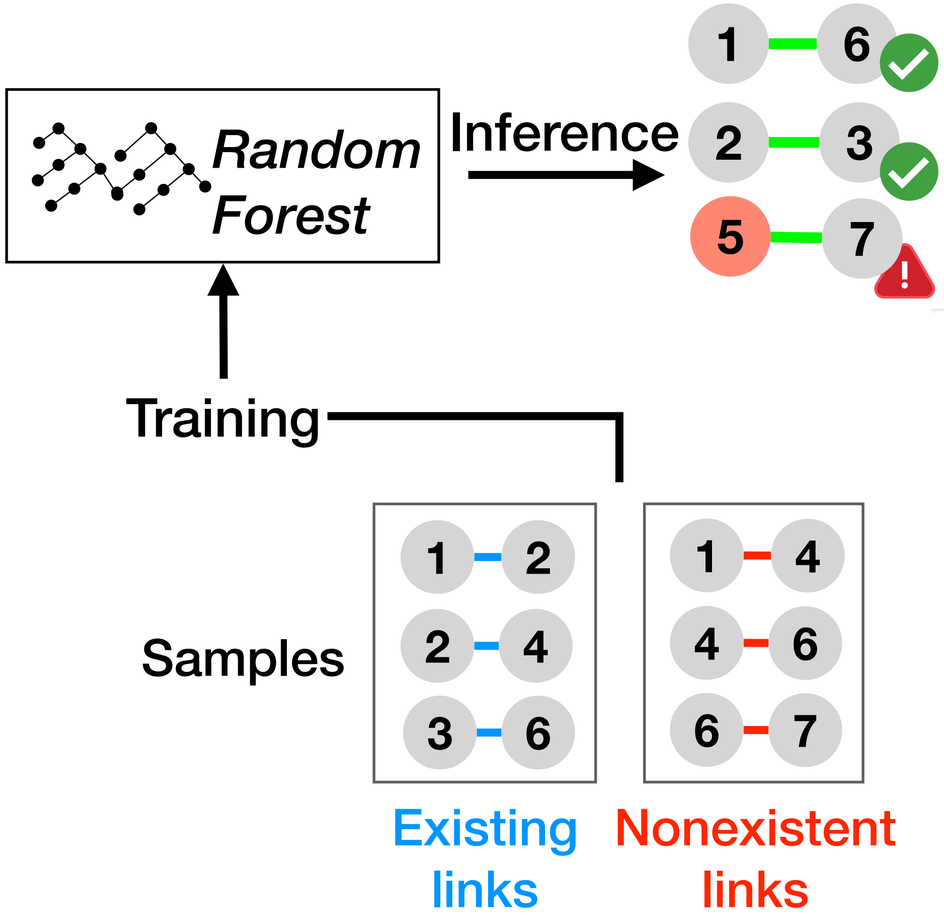




DFOH's fake AS links inference algorithm comprises three steps

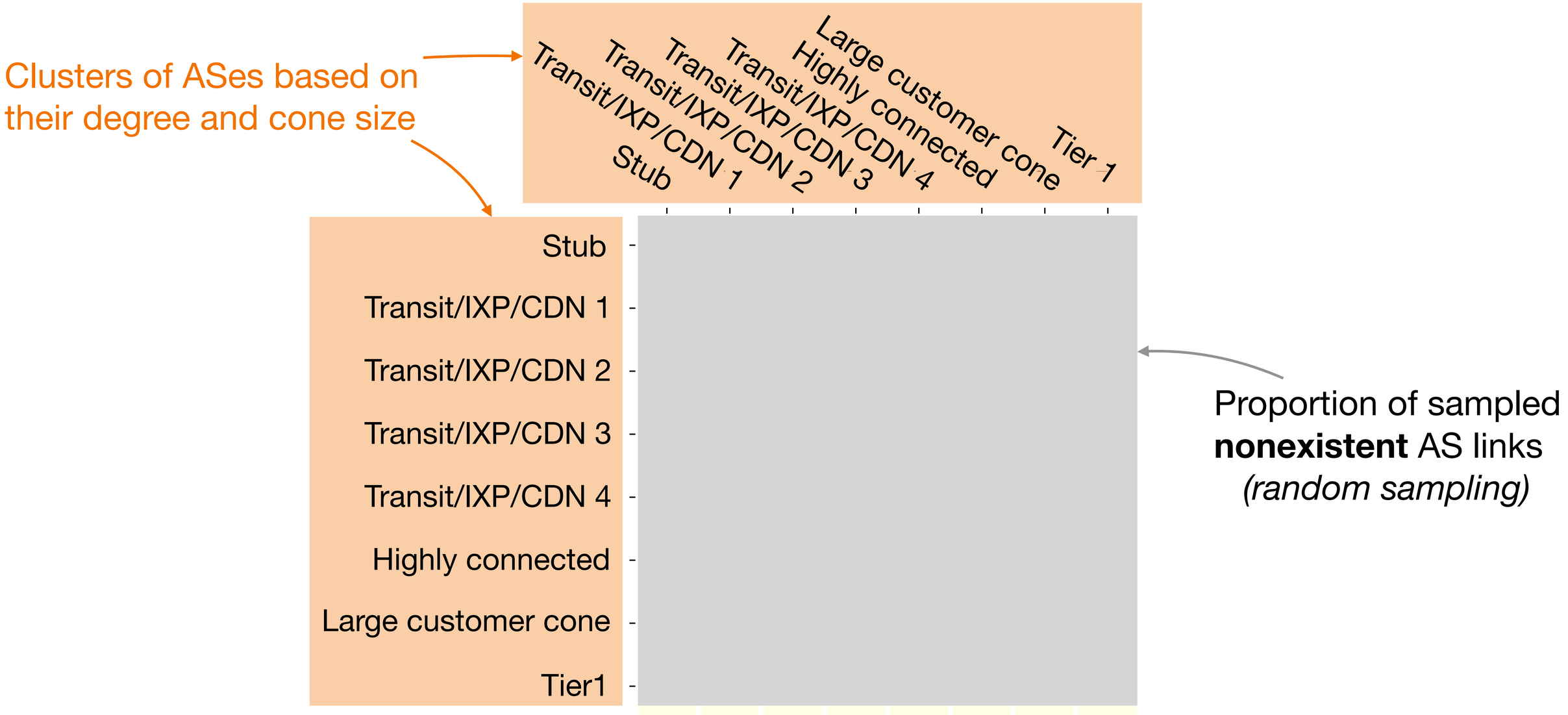






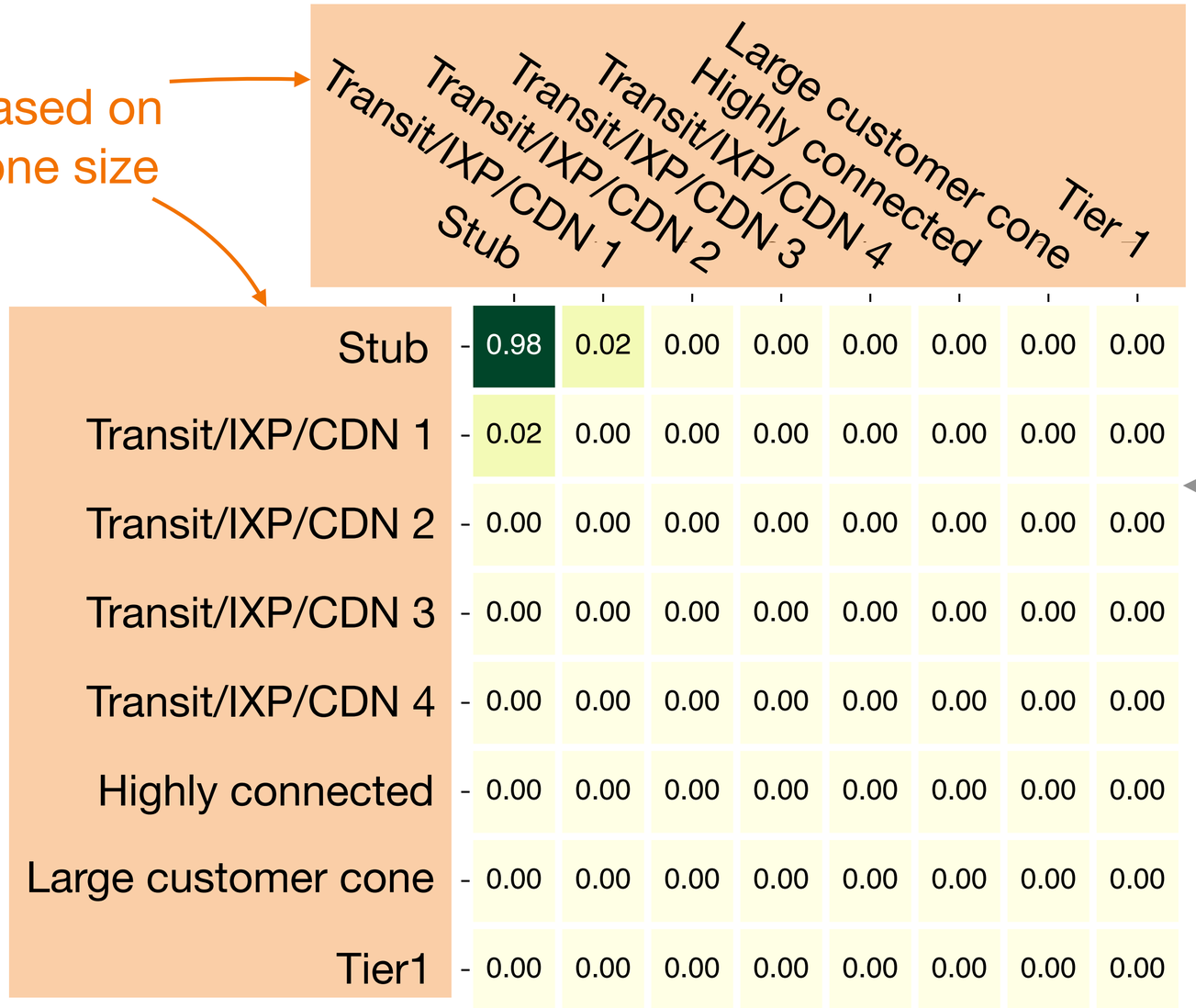
Problem: randomly sampling **nonexistent** links makes DFOH skewed towards stub-to-stub links as they are overrepresented

Problem: randomly sampling **nonexistent** links makes DFOH skewed towards stub-to-stub links as they are overrepresented



Problem: randomly sampling **nonexistent** links makes DFOH skewed towards stub-to-stub links as they are overrepresented

Clusters of ASes based on their degree and cone size



Proportion of sampled **nonexistent** AS links *(random sampling)*

Problem: randomly sampling **nonexistent** links makes DFOH skewed towards stub-to-stub links as they are overrepresented

DFOH would perform well on scenarios involving two stubs

Proportion of sampled **nonexistent** AS links *(random sampling)*

Problem: randomly sampling **nonexistent** links makes DFOH skewed towards stub-to-stub links as they are overrepresented

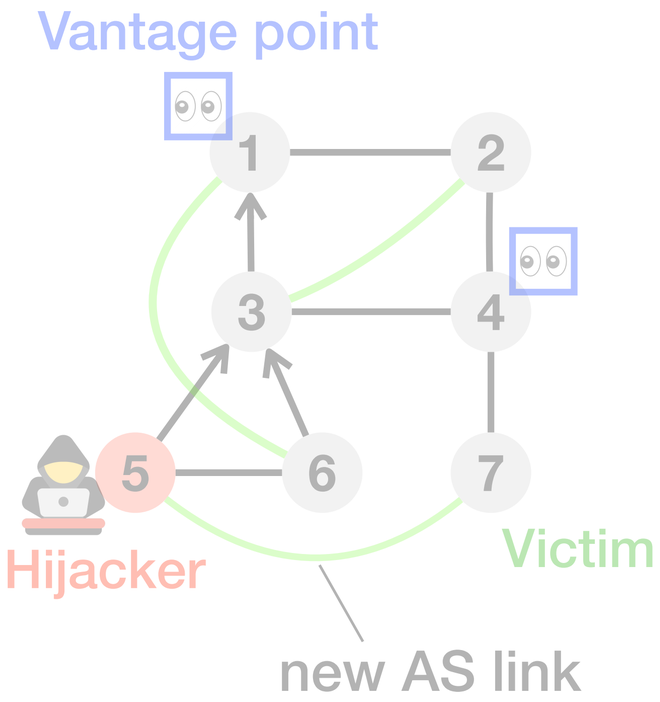
DFOH would perform well on scenarios involving two stubs

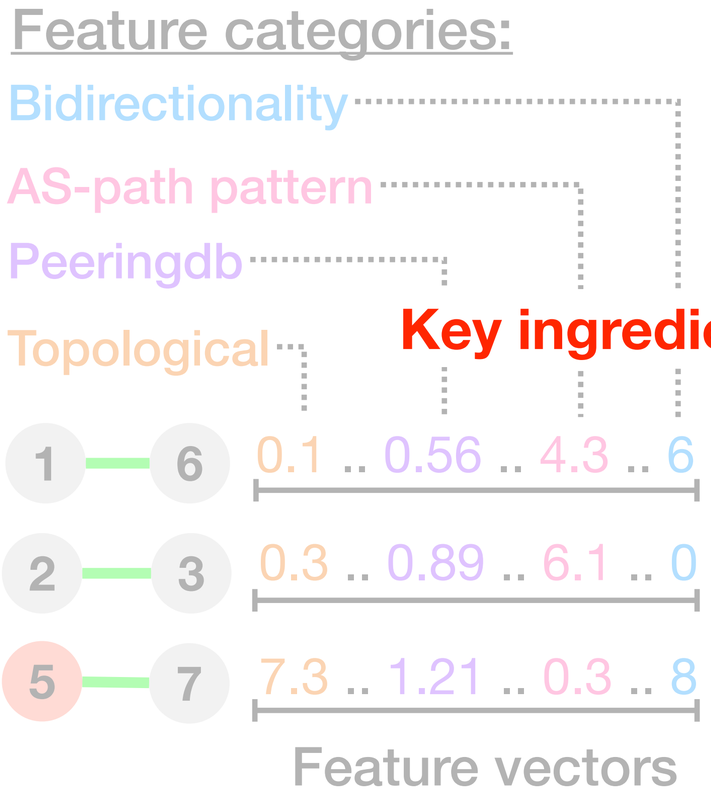
But not on the other scenarios

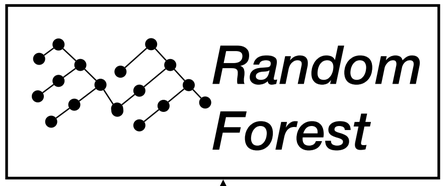
	Stub	Transit/IXP/CDN 1	Transit/IXP/CDN 2	Transit/IXP/CDN 3	Transit/IXP/CDN 4	Highly connected	Large customer cone	Tier1
Stub	0.98	0.02	0.00	0.00	0.00	0.00	0.00	0.00
Transit/IXP/CDN 1	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Transit/IXP/CDN 2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Transit/IXP/CDN 3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Transit/IXP/CDN 4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Highly connected	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Large customer cone	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Tier1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

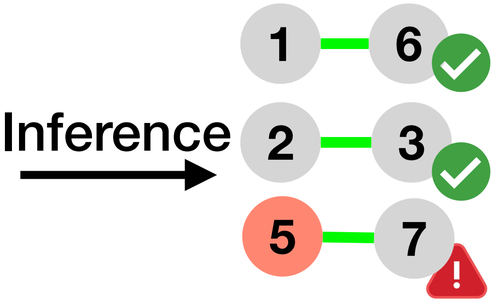
Proportion of sampled **nonexistent** AS links *(random sampling)*

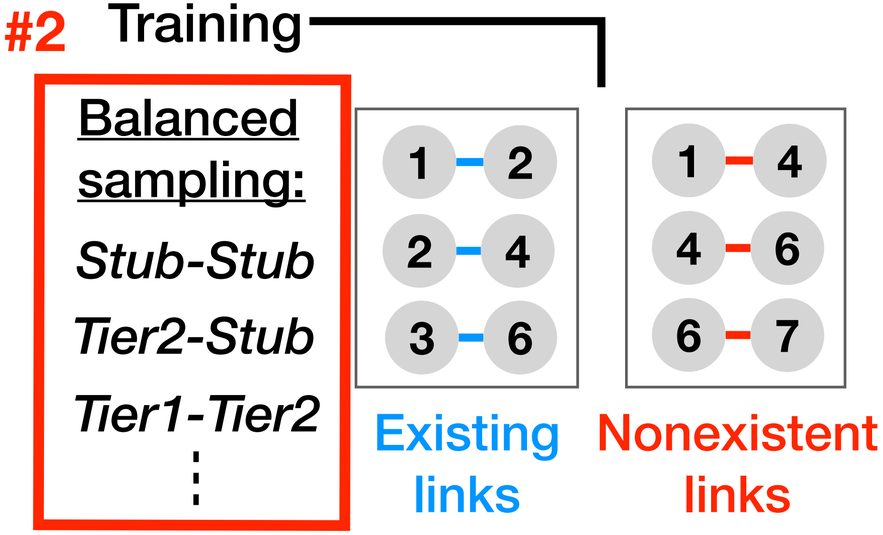
DFOH's fake AS links inference algorithm comprises three steps











Outline

DFOH's main challenge — is to detect fake AS links

DFOH's inference pipeline — discriminates fake AS links from the real ones

DFOH's inferences are accurate — in every attack scenario

DFOH is up and running

We evaluate ***DFOH*** on artificially created forged-origin hijacks and measure its accuracy upon every attack scenario

Methodology:

Step #1: We take existing AS paths
and prepend a new origin to create a new link

Step #2: We consider 9k cases where the new link exists (*legitimate cases*)
and 9k cases where the new link does not exist (*malicious cases*)

We evaluate ***DFOH*** on artificially created forged-origin hijacks and measure its accuracy upon every attack scenario

Methodology:

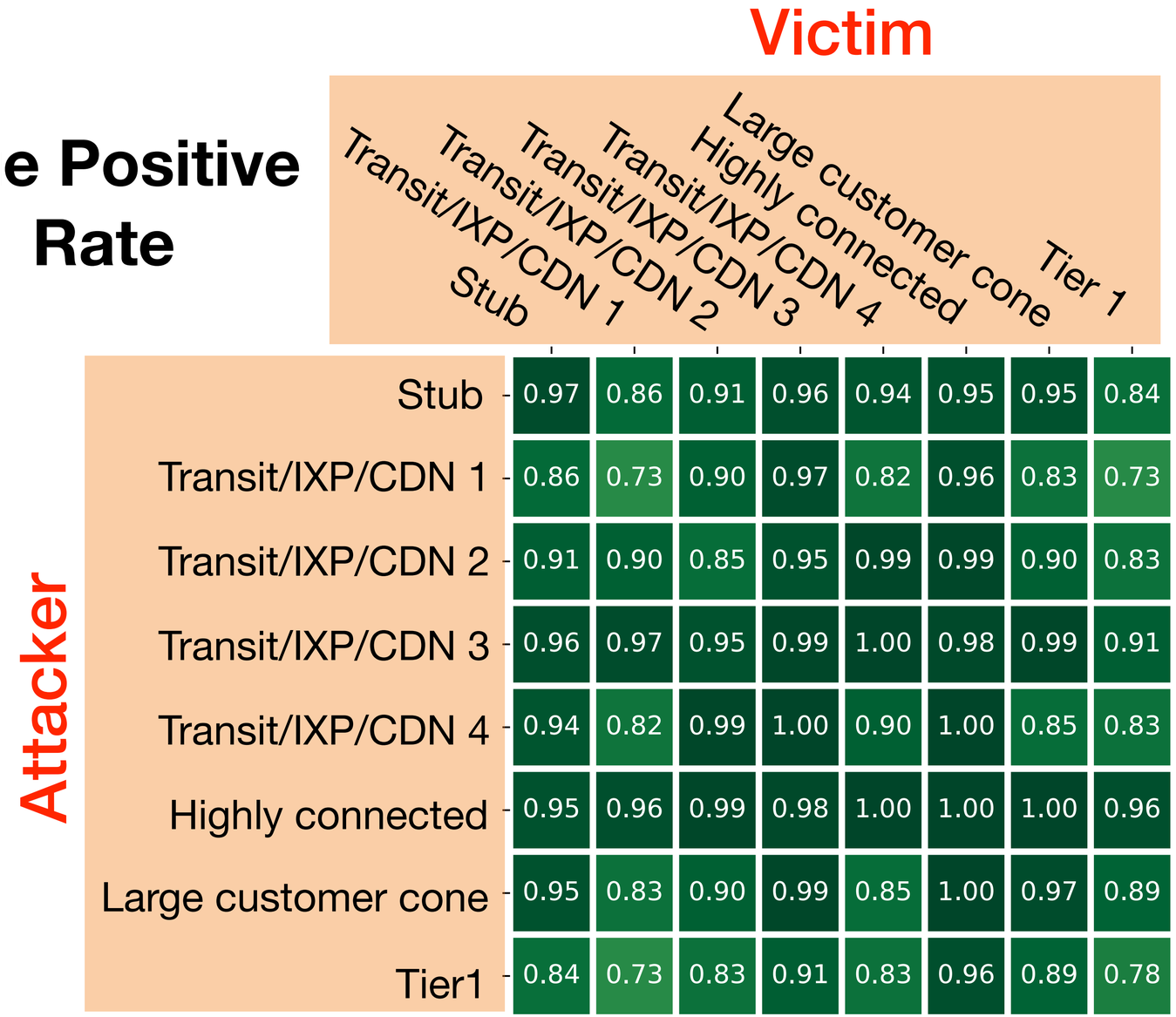
Step #1: We take existing AS paths
and prepend a new origin to create a new link

Step #2: We consider 9k cases where the new link exists (*legitimate cases*)
and 9k cases where the new link does not exist (*malicious cases*)

We focus on the **True Positive Rate** (TPR)
and the **False Positive Rate** (FPR)

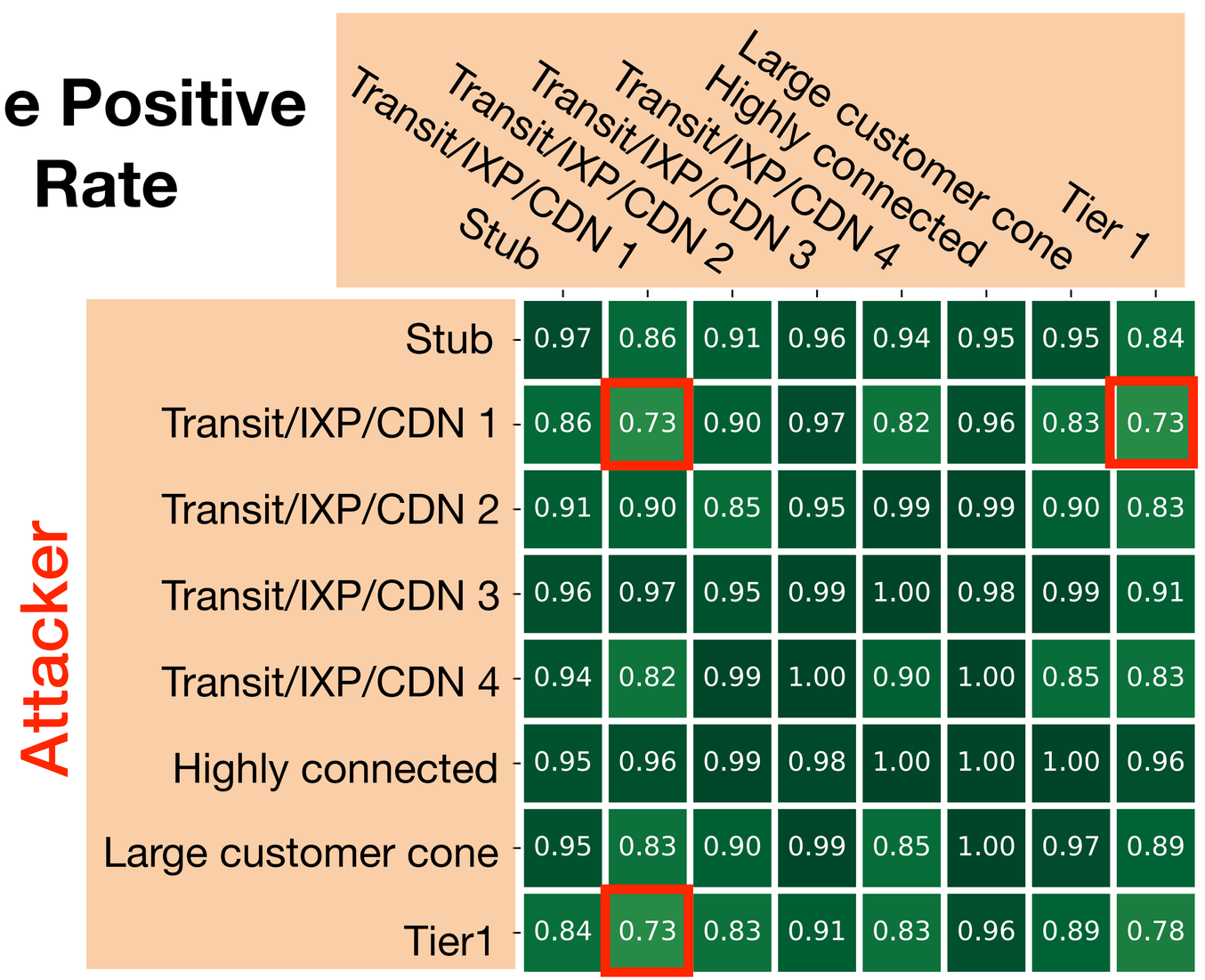
DFOH is accurate upon every attack scenario

True Positive Rate



DFOH is accurate upon every attack scenario

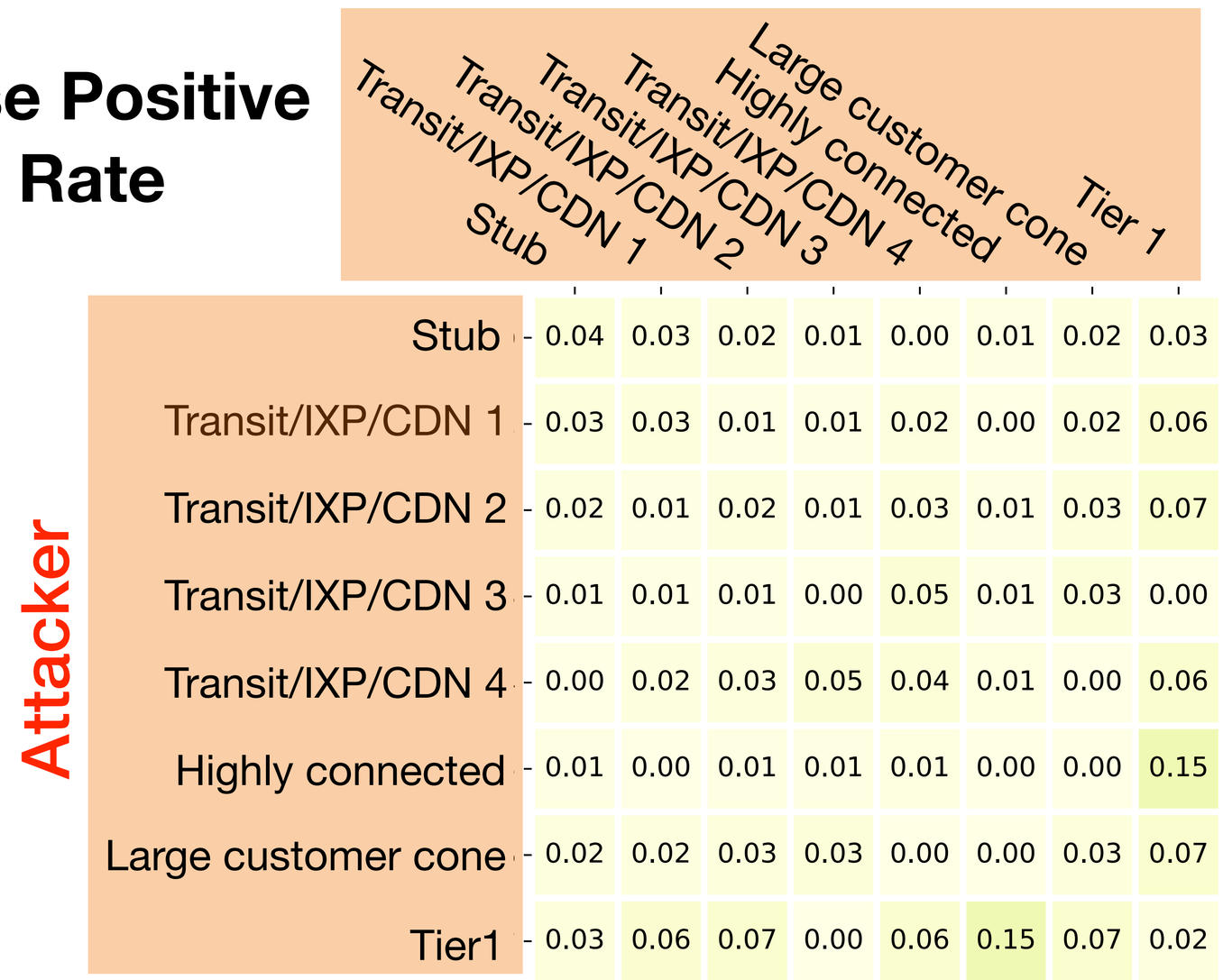
True Positive Rate



The minimum TPR is 0.73

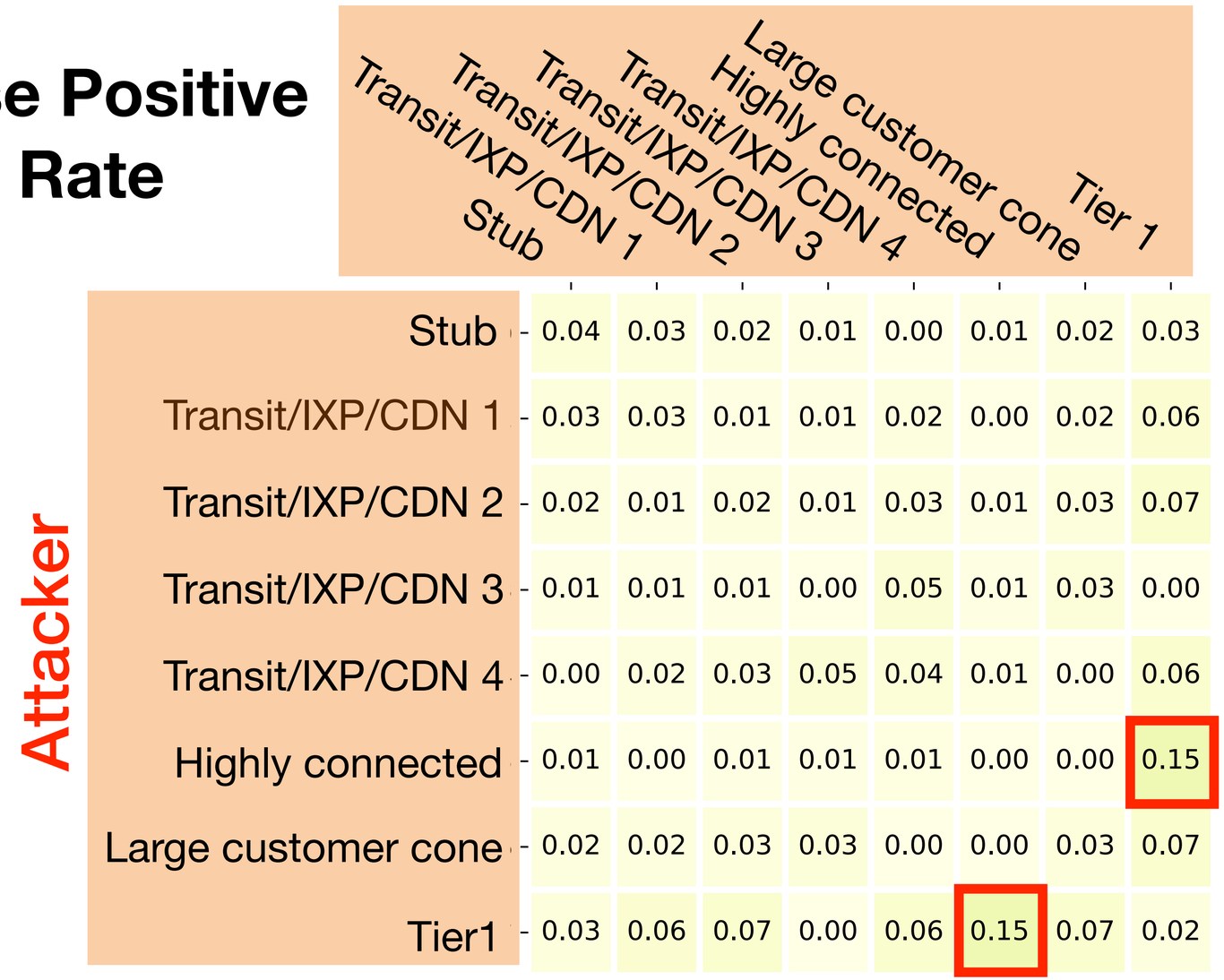
DFOH is accurate upon every attack scenario

False Positive Rate



DFOH is accurate upon every attack scenario

False Positive Rate



The maximum FPR is 0.15

Outline

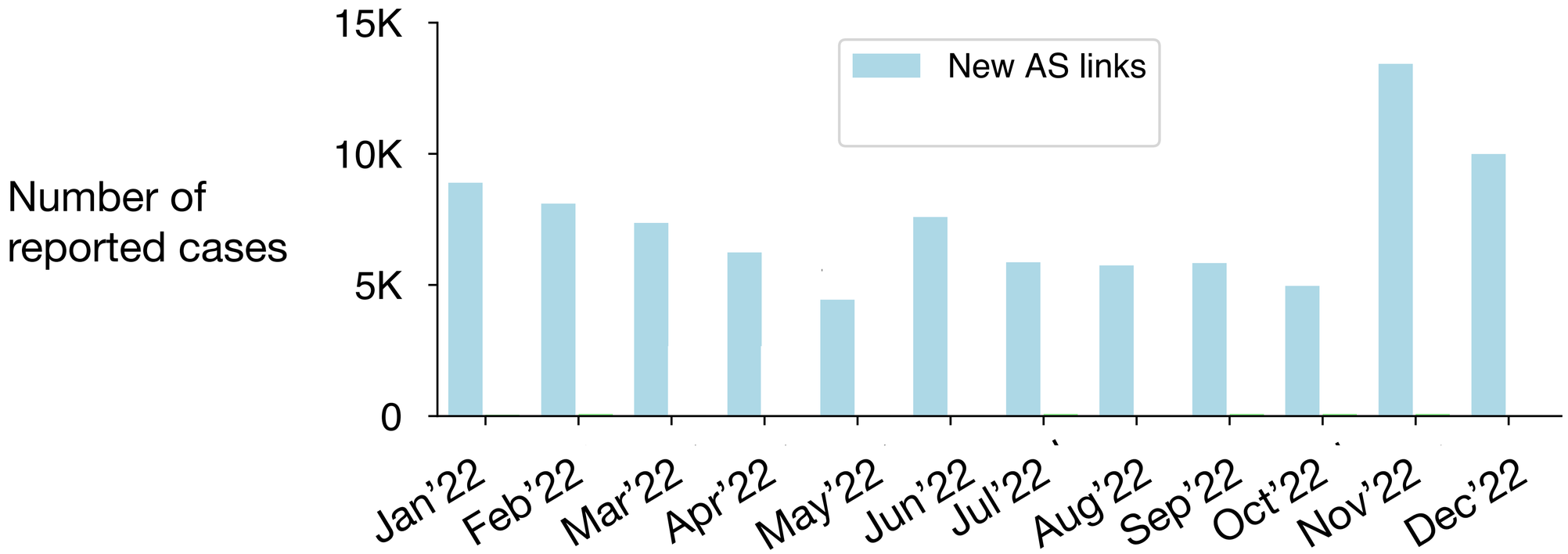
***DFOH*'s main challenge** is to detect fake AS links

***DFOH*'s inference pipeline** discriminates fake AS links from the real ones

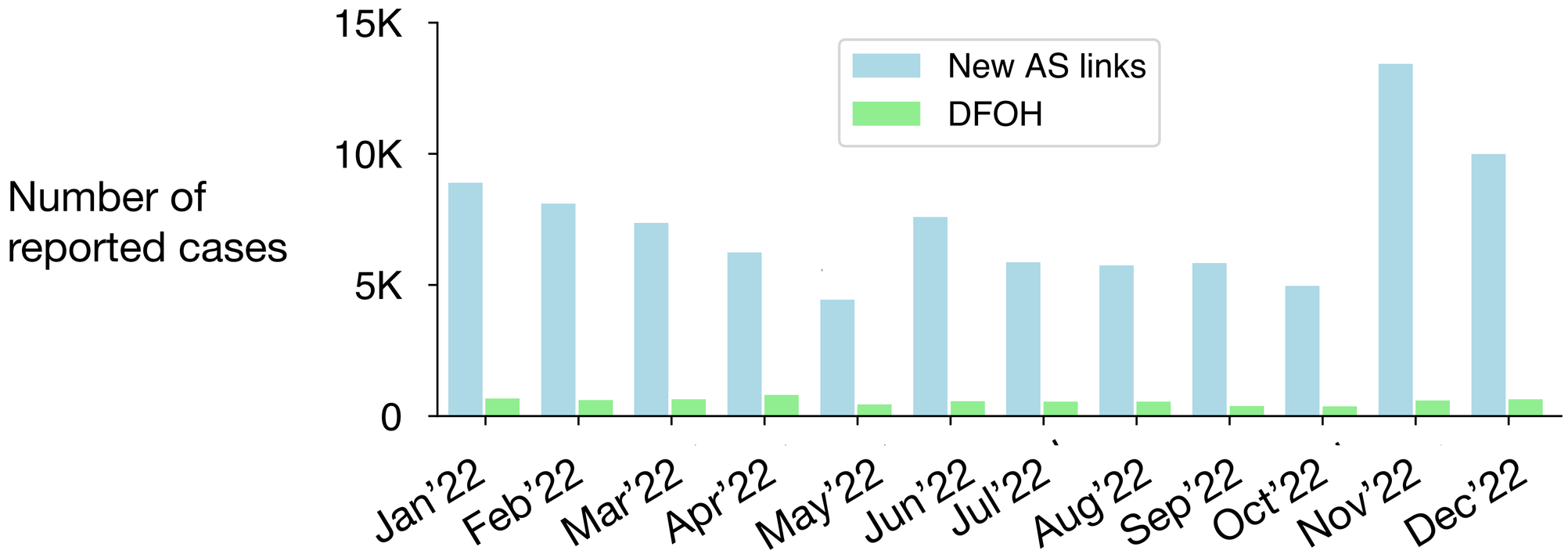
***DFOH*'s inferences are accurate** in every attack scenario

***DFOH is* up and running** and useful for operators

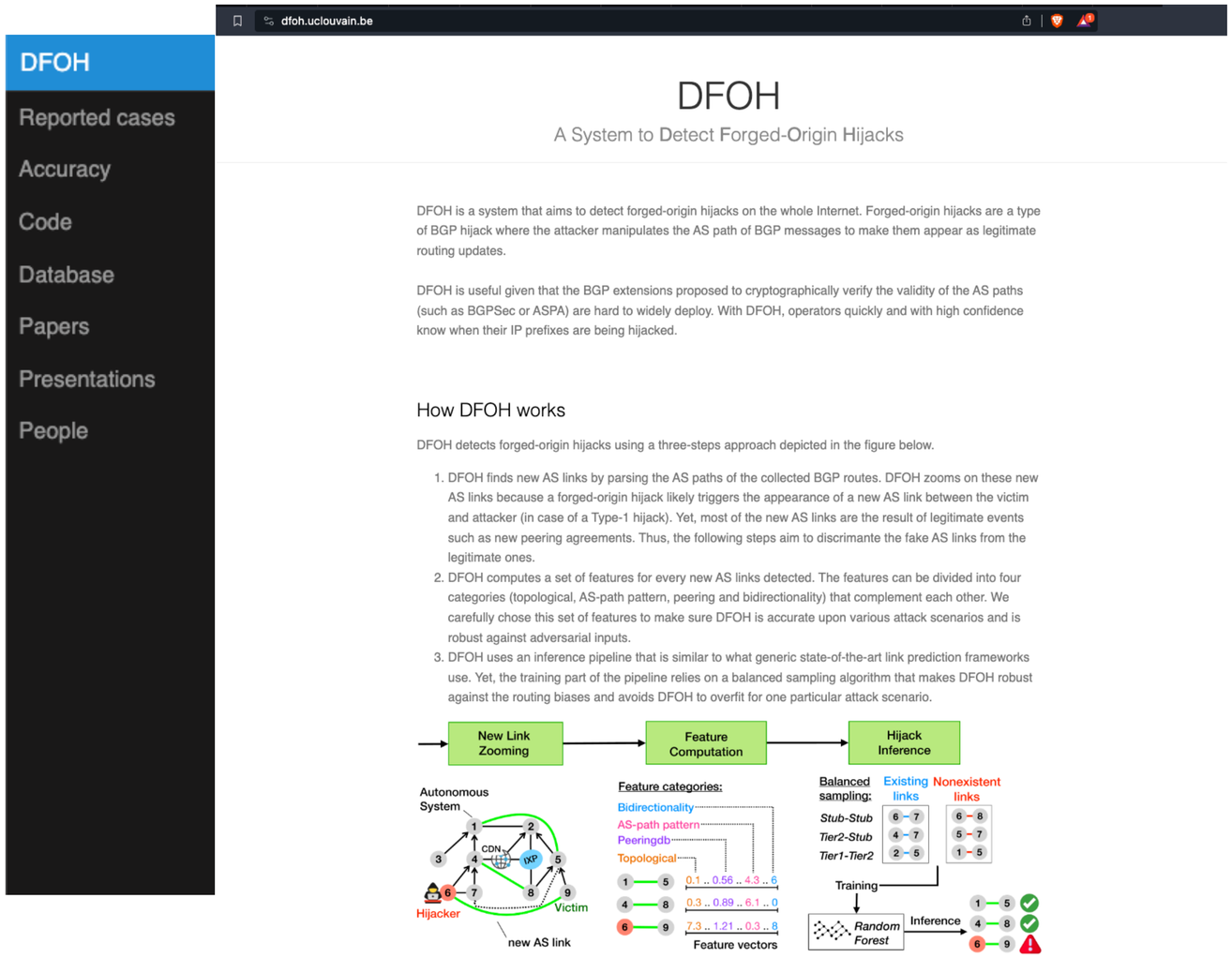
DFOH makes the detection of forged-origin hijacks practical for operators



DFOH makes the detection of forged-origin hijacks practical for operators

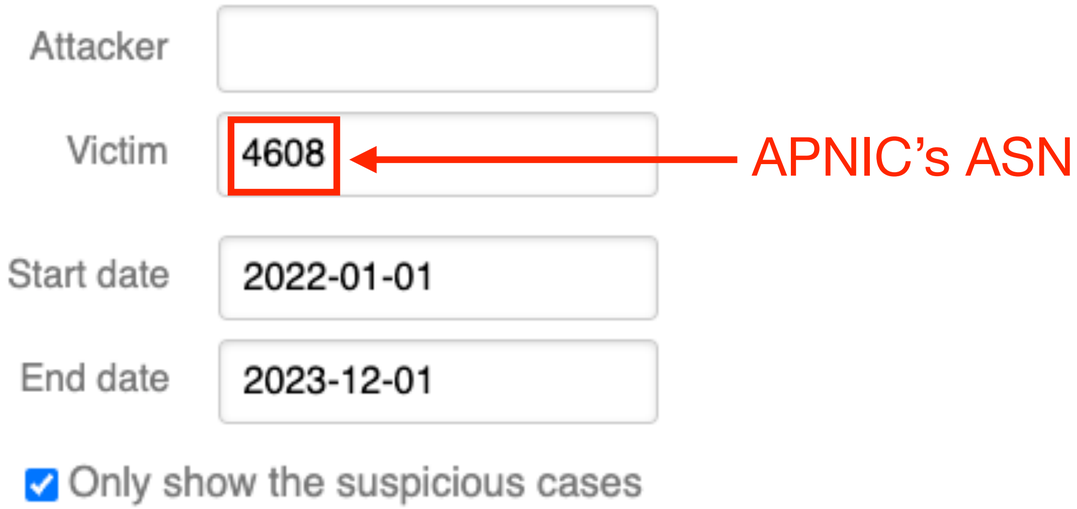


DFOH is up and running at https://dfoh.uclouvain.be/

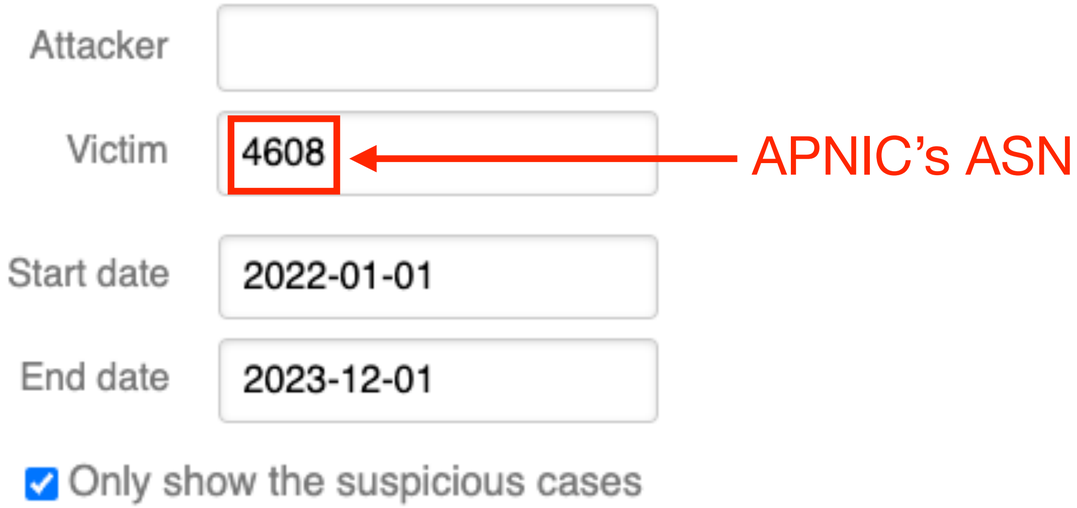


We provide the paper, presentations and source code

We showcase ***DFOH*** with APNIC's prefix and ASN!



We showcase *DFOH* with APNIC's prefix and ASN!



There suspicious cases reported over two years

Date	AS link	# of AS paths	DFOH inference	Confidence level
2022-07-10	*4608 147028*	1	suspicious	2
2022-07-22	*4608 9269*	1	suspicious	2
2022-07-25	*3257 4608*	27	suspicious	1

We showcase *DFOH* with APNIC's prefix and ASN!

Attacker

Victim 4608 ← APNIC's ASN

Start date 2022-01-01

End date 2023-12-01

☑ Only show the suspicious cases

There suspicious cases reported over two years

Date	AS link	# of AS paths	DFOH inference	Confidence level
2022-07-10	*4608 147028*	1	suspicious	2
2022-07-22	*4608 9269*	1	suspicious	2
2022-07-25	*3257 4608*	27	suspicious	1

Time	Prefix	AS path	Vantage points
2022-07-10 07:12:37	*103.0.0.0/16*	*44393 147028 4608*	*RRC00 49.12.70.222*

We showcase *DFOH* with APNIC's prefix and ASN!

Attacker

Victim 4608 ← APNIC's ASN

Start date 2022-01-01

End date 2023-12-01

☑ Only show the suspicious cases

There suspicious cases reported over two years

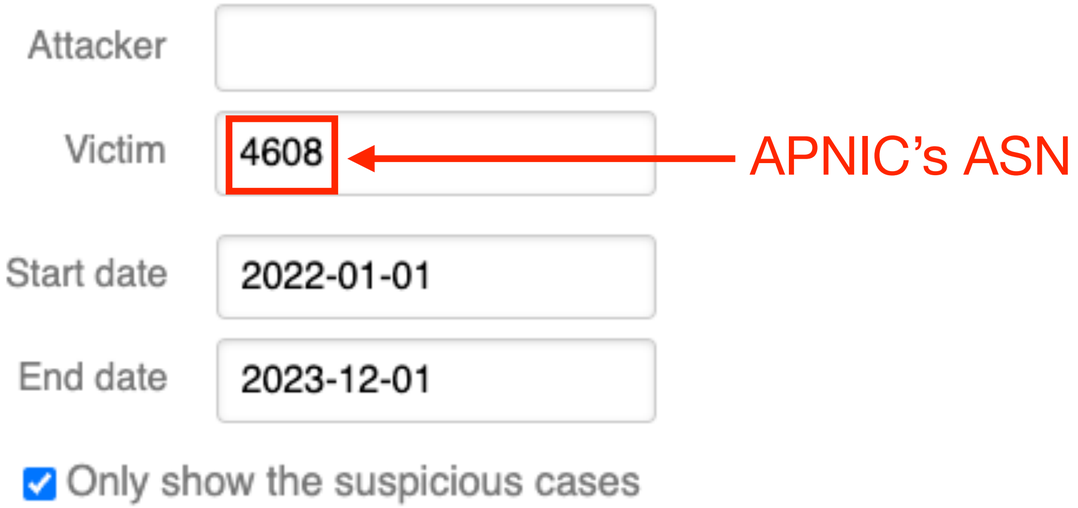
Date	AS link	# of AS paths	DFOH inference	Confidence level
2022-07-10	*4608 147028*	1	suspicious	2
2022-07-22	*4608 9269*	1	suspicious	2
2022-07-25	*3257 4608*	27	suspicious	1

APNIC's Prefix

Time	Prefix	AS path	Vantage points
2022-07-10 07:12:37	*103.0.0.0/16*	*44393 147028 4608*	*RRC00 49.12.70.222*

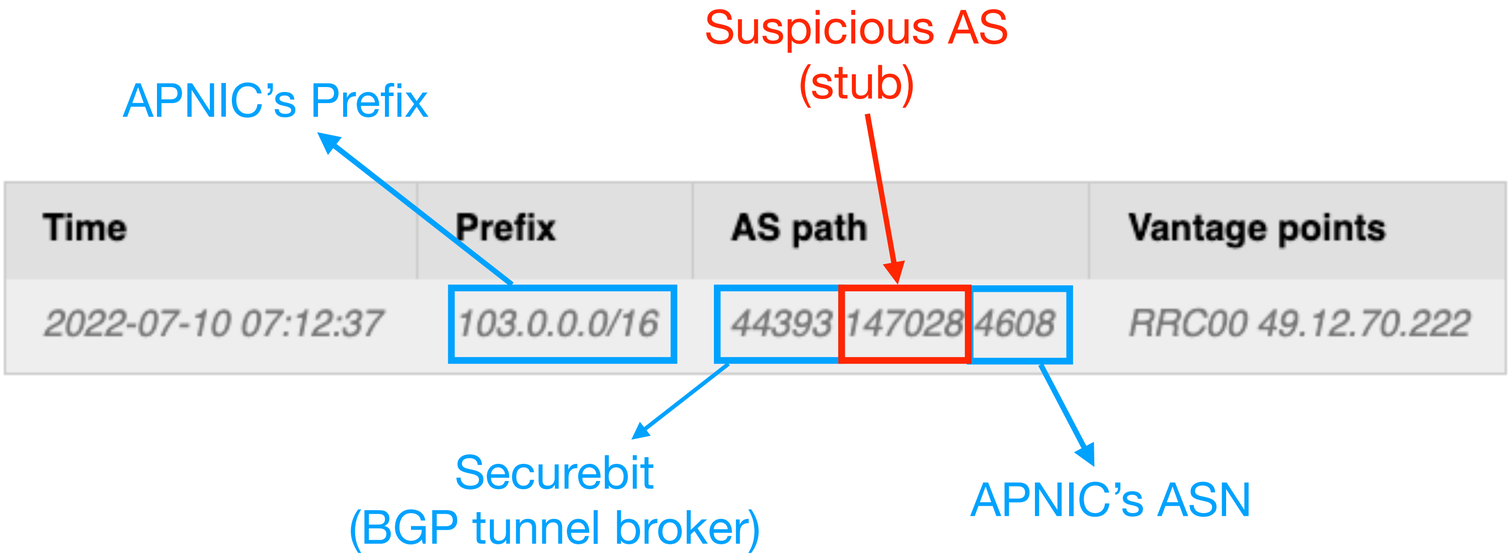
APNIC's ASN

We showcase *DFOH* with APNIC's prefix and ASN!



There suspicious cases reported over two years

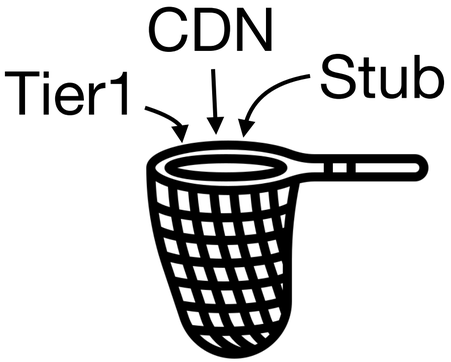
Date	AS link	# of AS paths	DFOH inference	Confidence level
2022-07-10	*4608 147028*	1	suspicious	2
2022-07-22	*4608 9269*	1	suspicious	2
2022-07-25	*3257 4608*	27	suspicious	1



DFOH: A System to Detect Forged-Origin Hijacks

DFOH runs in a commodity server

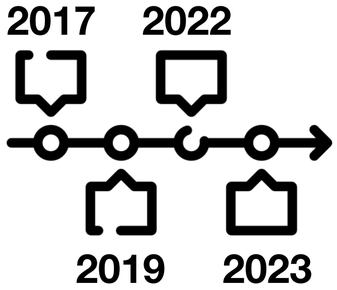
DFOH detects hijacks on the whole Internet



DFOH is accurate in every attack scenario

DFOH: A System to Detect Forged-Origin Hijacks

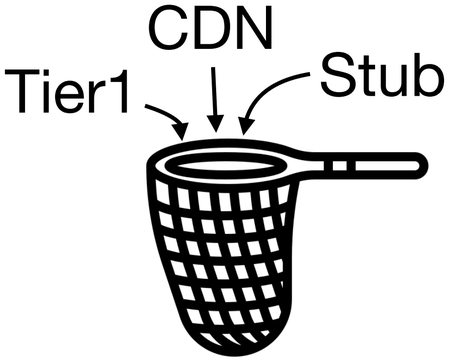
DFOH runs in a commodity server



DFOH detects past hijacks

DFOH detects hijacks on the whole Internet

DFOH provides near-real-time detection



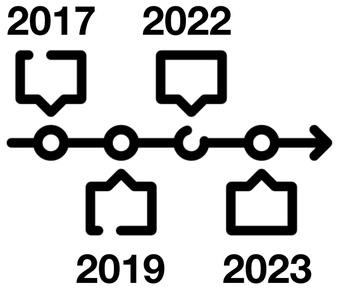
DFOH is accurate in every attack scenario

DFOH is robust against adversarial inputs

DFOH: A System to Detect Forged-Origin Hijacks

https://dfoh.uclouvain.be

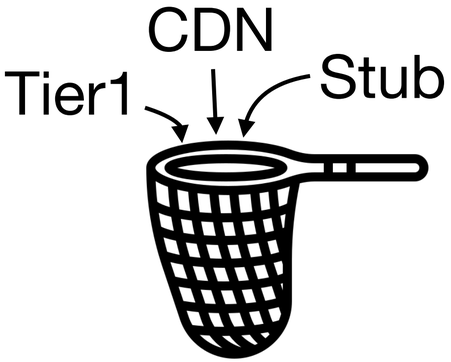
DFOH runs in a commodity server



DFOH detects past hijacks

DFOH detects hijacks on the whole Internet

DFOH provides near-real-time detection



DFOH is accurate in every attack scenario

DFOH is robust against adversarial inputs