Detecting Fake AS-PATHs based on Link Prediction

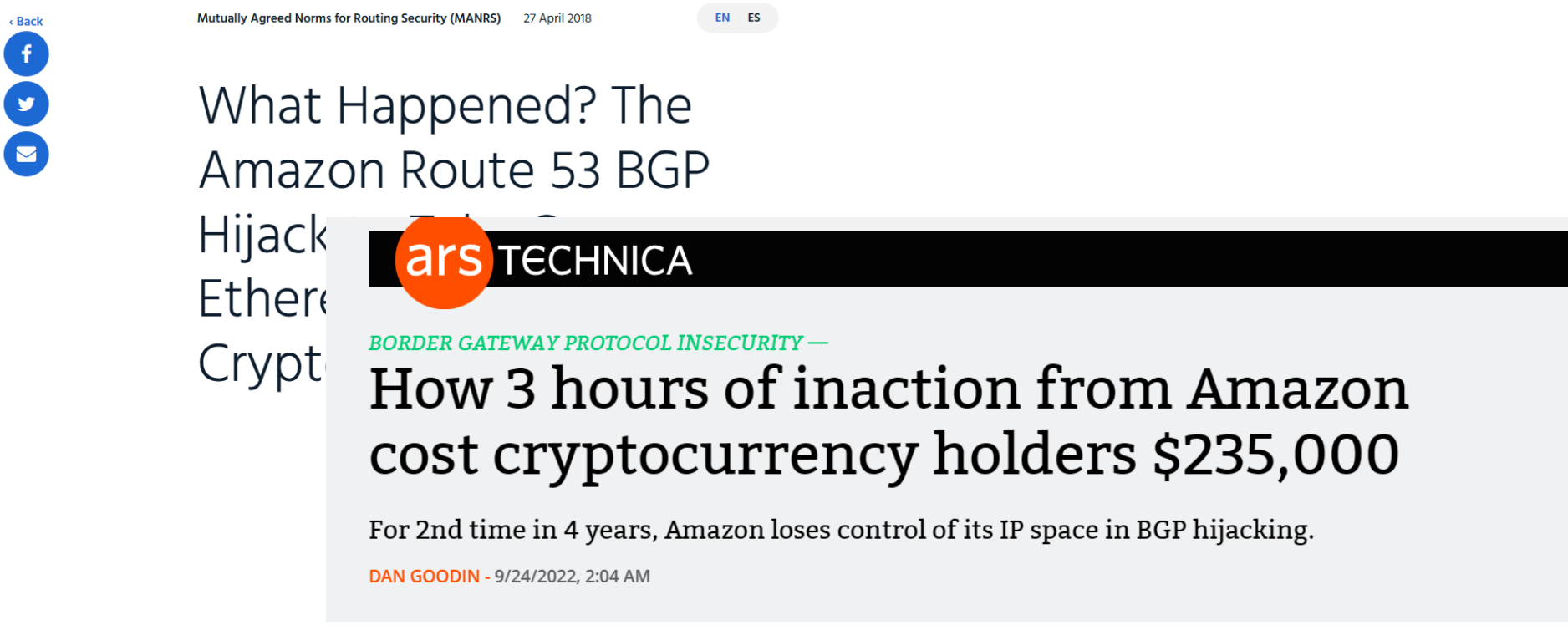
Accepted by ISCC2023

Chengwan Zhang

2023.5.24

BGP hijacking

- BGP hijacking refers to the behavior of an attacker who redirects traffic by injecting bogus routing information.



BGP hijacking

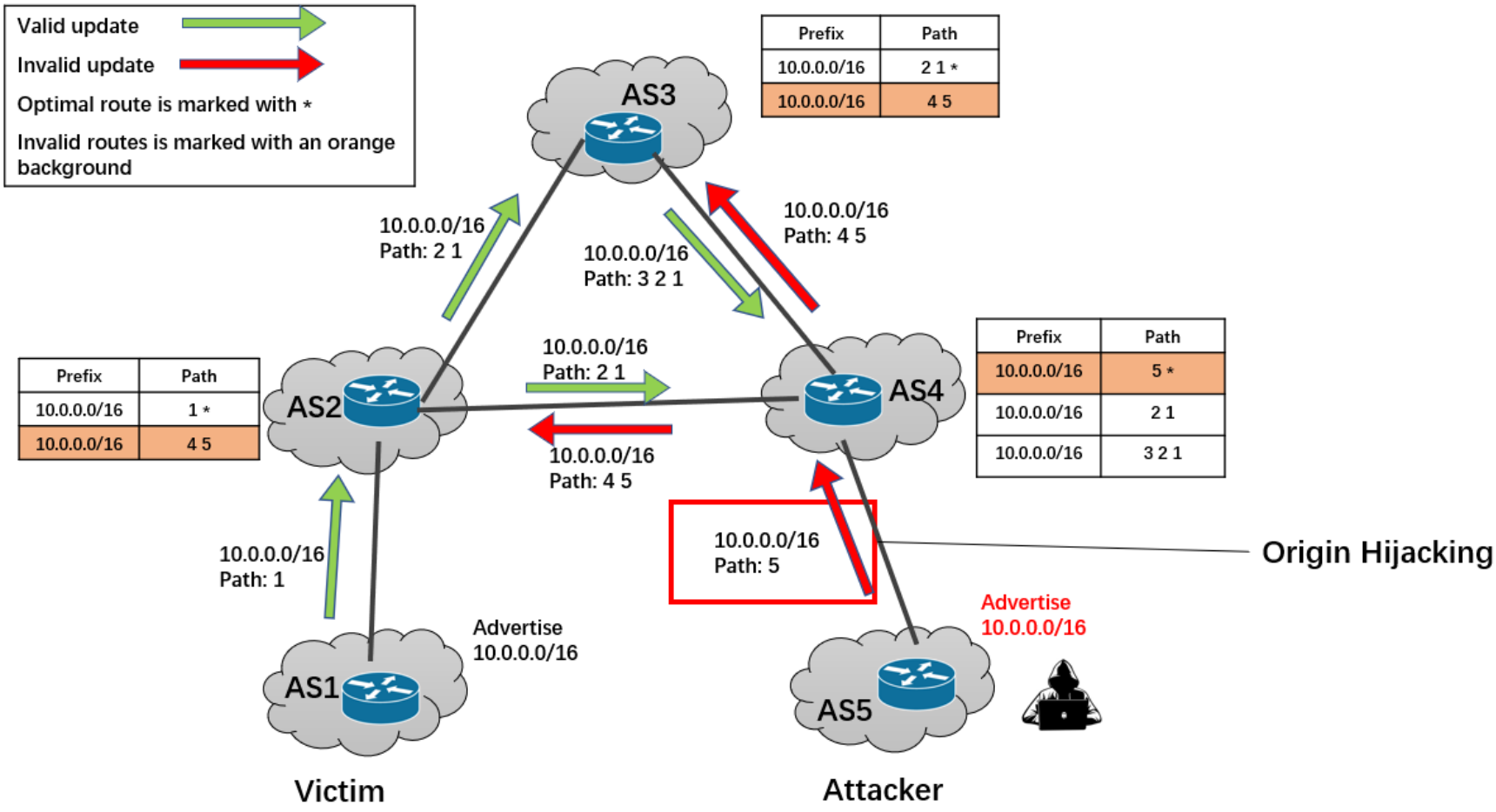
- Origin hijacking: the attacker AS directly originates the victim’ s IP prefix.
- Path hijacking: The attacker manipulates the AS-PATH before announcing the victim's IP prefix.

```
TIME: 05/13/03 00:01:45
TYPE: BGP4MP/MESSAGE/Update
FROM: 134.55.20.229 AS293
TO: 198.32.162.102 AS6447
WITHDRAW
  195.69.188.0/22
  198.153.20.0/22
  203.130.204.0/24

TIME: 05/13/03 00:01:45
TYPE: BGP4MP/MESSAGE/Update
FROM: 134.55.20.229 AS293
TO: 198.32.162.102 AS6447
ORIGIN: IGP
ASPATH: 293 1239 9405 4538
NEXT_HOP: 134.55.20.229
ATOMIC_AGGREGATE
AGGREGATOR: AS4538 202.112.60.250
ANNOUNCE
  219.216.0.0/14
```

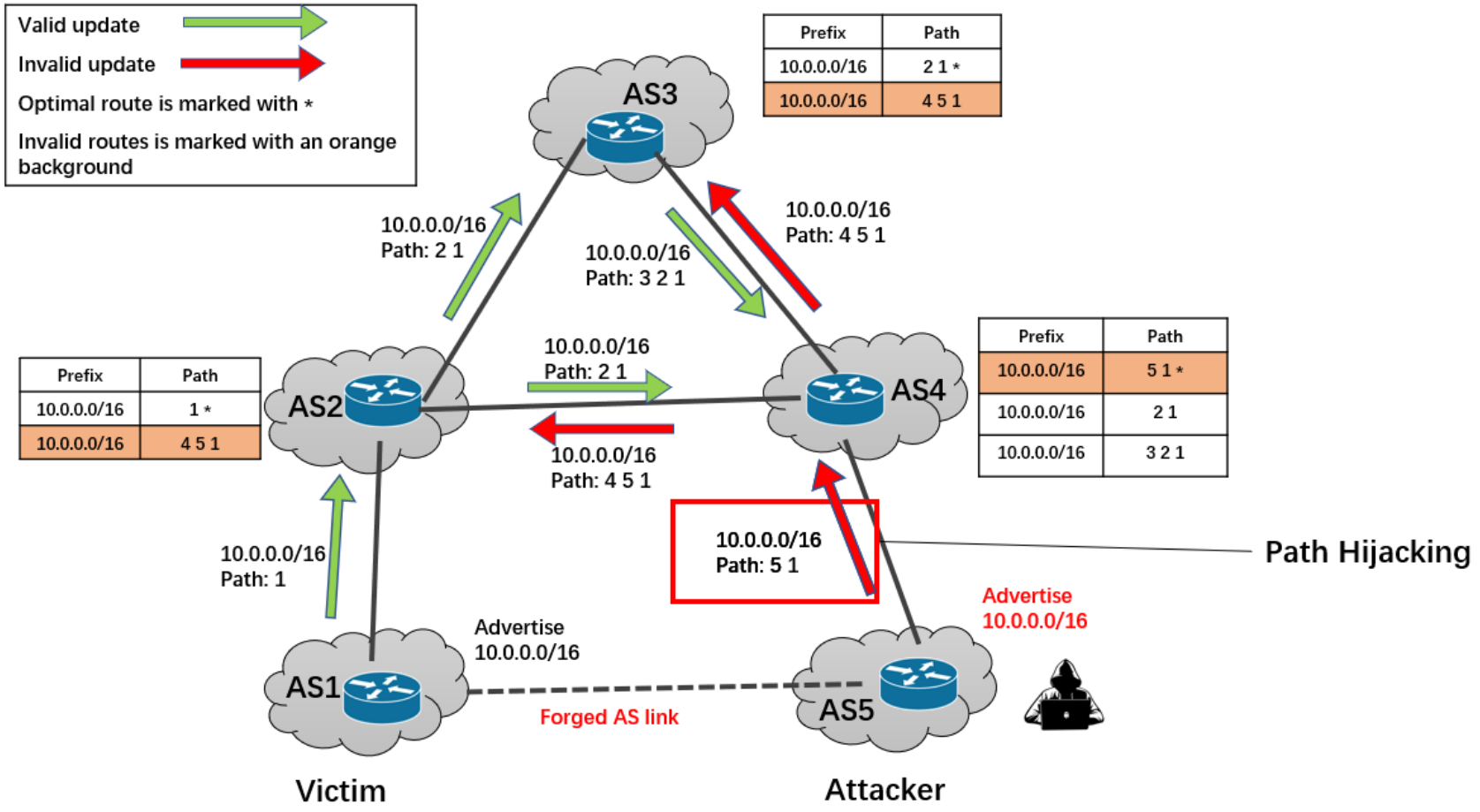
Origin Hijacking

- Origin hijacking will cause MOAS（Multi-Origin AS) conflict.



Path hijacking

- Path hijacking can evade MOAS ,but usually cause unseen AS link.

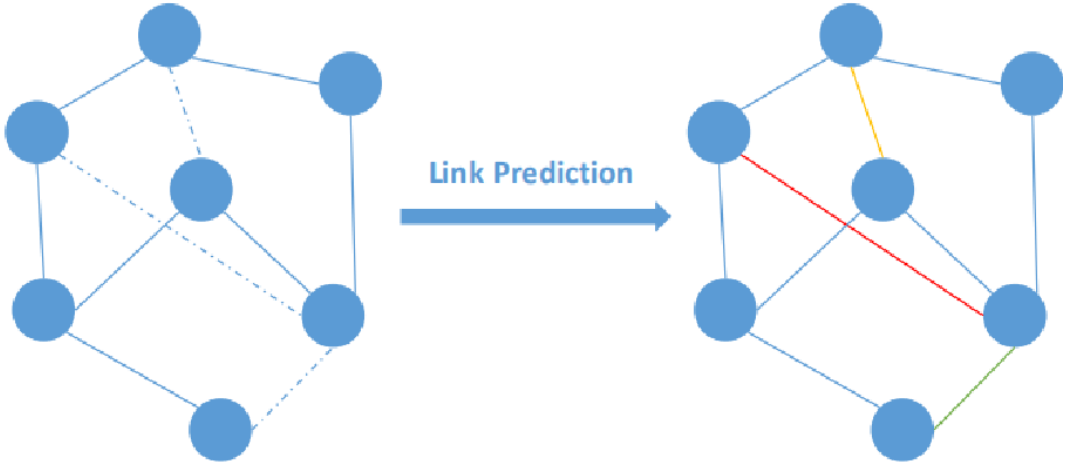


State-of-the-art for path hijacking detection

- Hybrid-plane detection technique（Argus、Fingerprints etc）
  - Treat **all unseen links** appearing in the control plane as suspicious event, then validate the event through the data-plane probing.
- Limitation
  - Unseen links are very common（New peering establishment, Backup links. Route policy changes, etc），and only a few of them are due to path hijacking.
  - Existing methods encounter severe data-plane overhead waste, making them Inefficient and difficult to guarantee real-time.

Idea

- Evaluating the authenticity of unseen links with link prediction and filtering the benign unseen links.
- Link prediction: a technique for inferring whether a link is likely to exist between two nodes from an existing observable portion of the network.



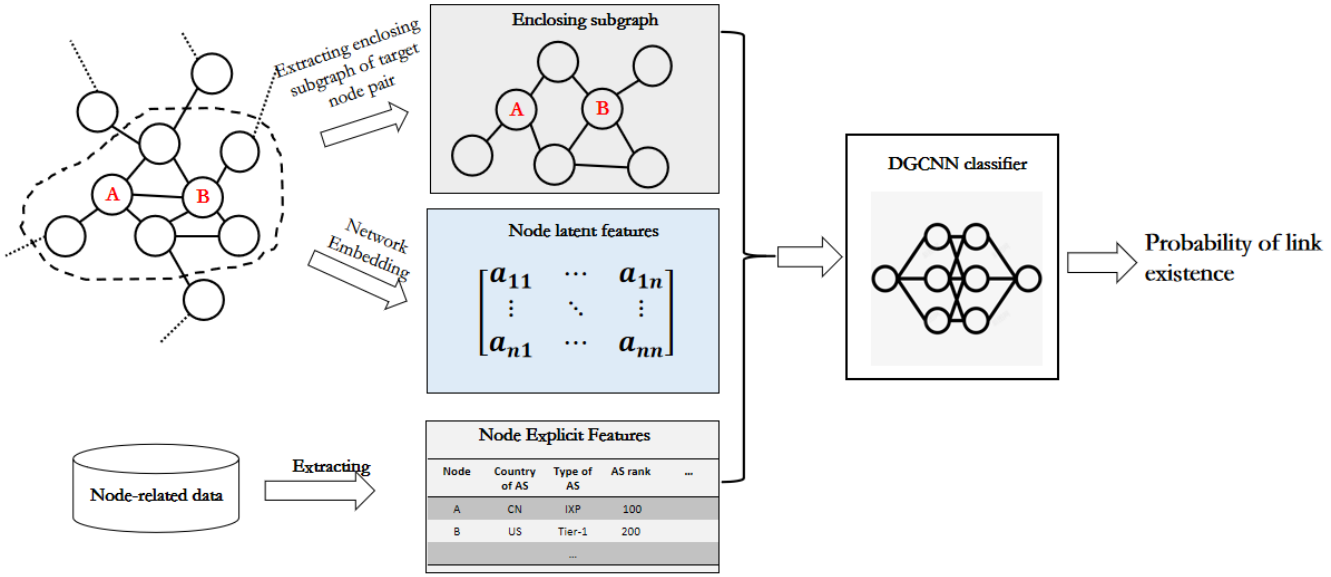
Is AS link predictable?

- Zhuang et al recently formulate the link prediction as a matrix completion task. Their work explain the predictability of AS link.

- Graph characteristics of AS-level topology
  - power-law distribution
  - negative degree-degree correlation
  - Hierarchical
  - AS links usually connect two ASes with the same properties.

Unseen link classification

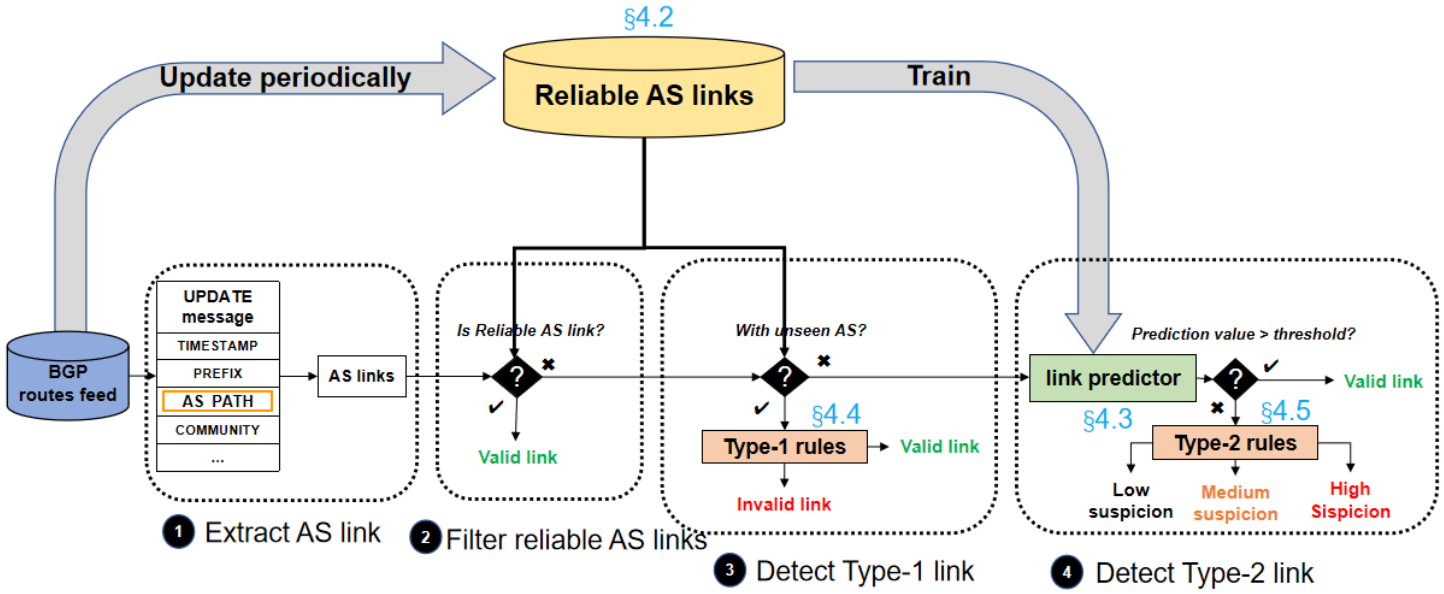
- We select SEAL as the link prediction algorithm
- CAIDA AS relationship 2021 & AS location、 type and size
- Training with positive and negative samples
- The accuracy reached 0.95 and the AUC reached 0.98



Workflow of SEAL

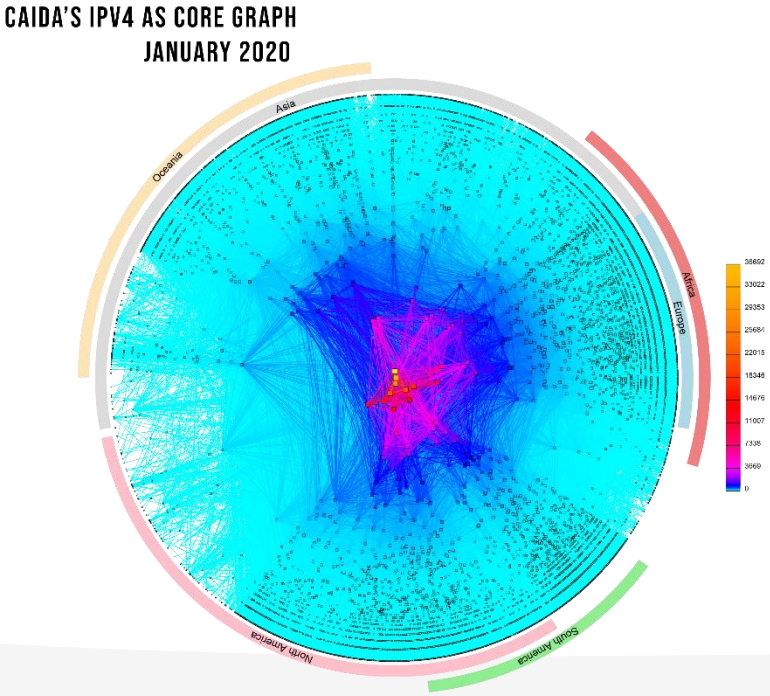
Metis: a fake AS-PATHs detection framework

- Still based on unseen links
- Combine link prediction and rules
- Link prediction is used to find suspicious unseen links, and rules are used to improve the confidence level



Reliable links

- Links are believed to be real links on the current AS topology
- Goal: more historical seen links but few obsolete links
- Our method: union of the past 6 months of the CAIDA AS relationship dataset



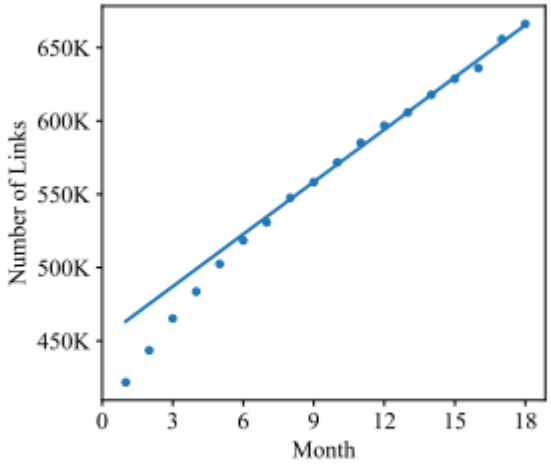
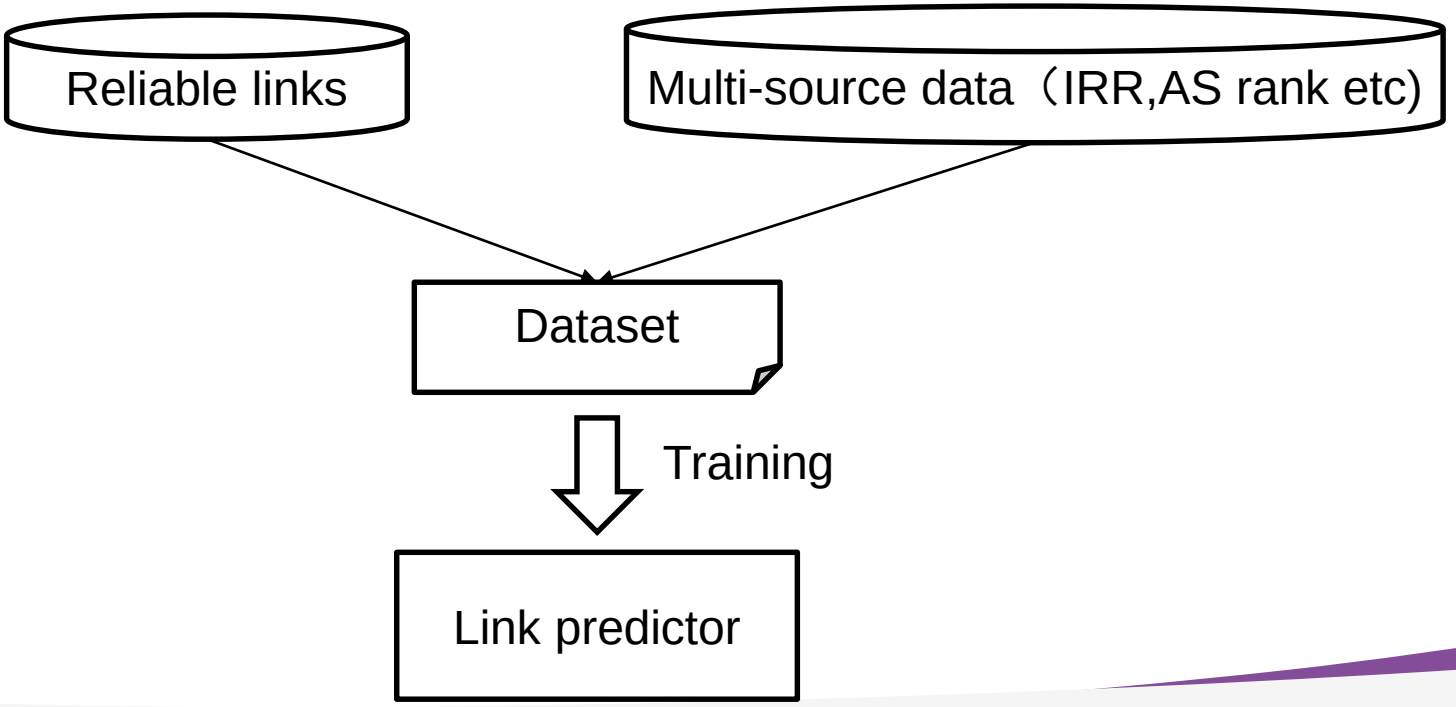


Fig. 7: The number of union AS links in CAIDA AS relationship data of the past N months of November 2021

Link predictor

- To evaluating the authenticity of unseen links
- Trained with reliable links and side information of ASes
- In the framework, it can use any link prediction algorithm

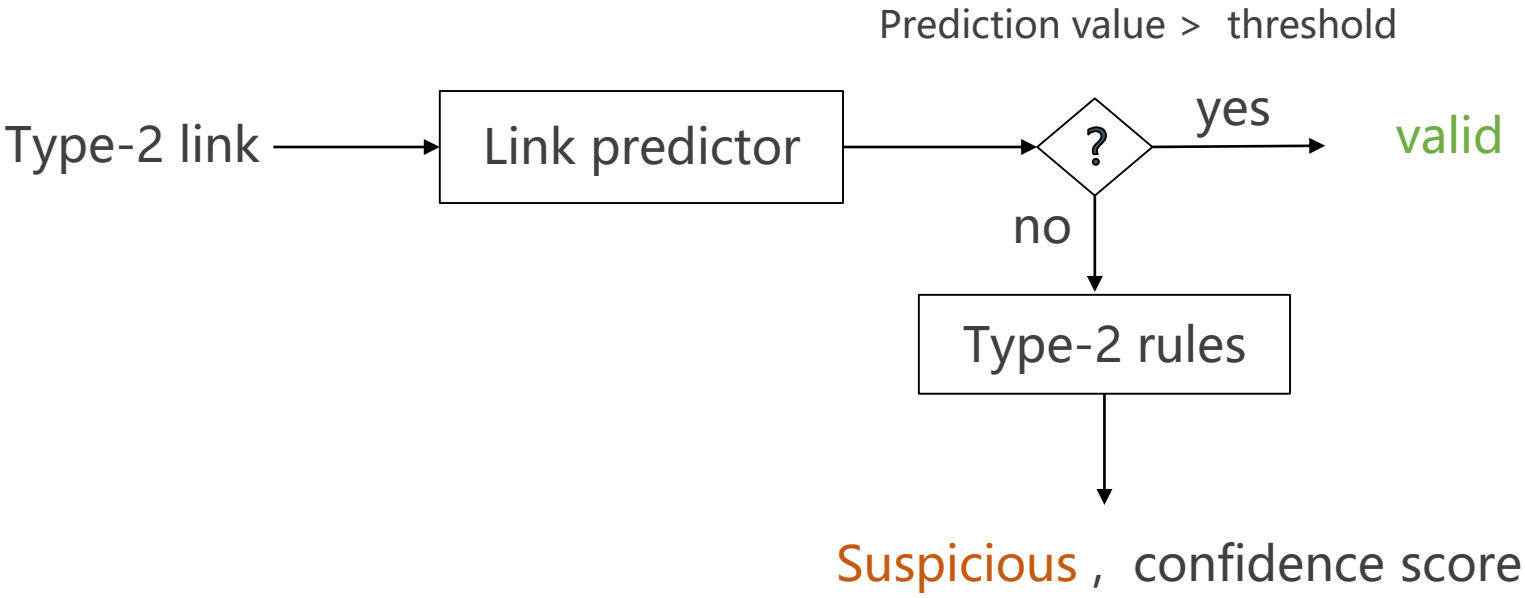


Type-1 unseen link detection

- Type-1 link with unseen new AS, cannot be evaluated by link predictor
- account for a relatively small percentage
- 3 simple rules:
  - The new AS is a reserved ASN
    - 24514 24490 24489 23911 4538 65534
  - The new AS is not registered in the whois data of the 5 RIRs
    - 24514 24490 24489 23911 4538 66666
  - The new AS is not the last hop in the AS-PATH (Our measurement show more than 97% of newly used ASes appear on the Internet as a stub AS.)
    - 24514 24490 24489 23911 4537 4538

Type-2 unseen link detection

- Input into link predictor, and then determine the confidence level with Type-2 rules.



Type-2 rules

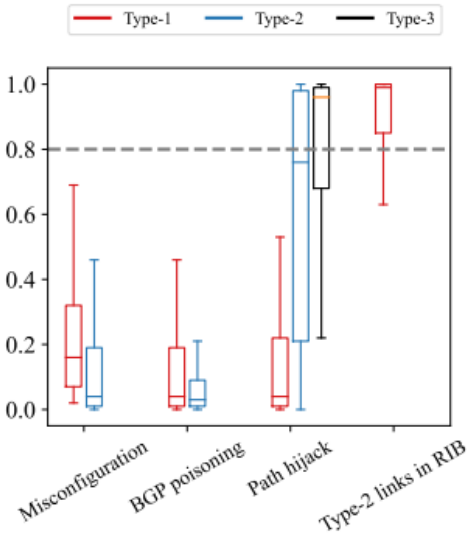
- Initial confidence score is 0
- The score increases 1 when:
  - AS-PATH is longer than the pre-set length threshold
  - The link with single digit ASN in the right side
  - The edit distance of the ASes is 1
  - Loop in AS-PATH, and the link is in the loop
  - AS-PATH violate valley-free rule
  - Traffic detour in the AS-PATH
- The score reduced by 2 when:
  - The suspicious link is at the end of the AS-PATH and the link is a domestic link

Evaluation

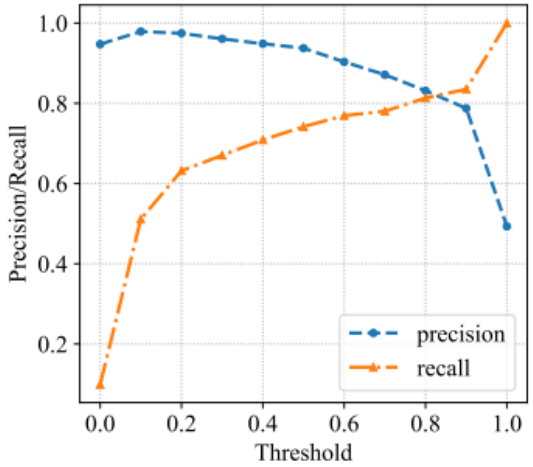
- Dataset
  - 7000 AS-PATHs in the RIB of RIPE RRC00 at 00:00 UTC on November 1, 2021
  - Misconfiguration
    - 24514 24490 24489 23911 4538 3
    - 24514 24490 24489 23911 4538 4528
  - BGP Poisoning
    - 24514 24490 24489 23911 4538 123 4538
    - 24514 24490 24489 23911 4538 123 456 4538
  - Path hijacking
    - 24514 24490 24489 23911 4538 16509
    - 24514 24490 24489 23911 4538 3356 16509

Evaluation

- Prediction values of crafted Type-2 links are significantly lower than that of the normal links in the RIB
- When the threshold is 0.8, the classification accuracy and recall are around 80%



(a)



(b)

Evaluation

- The accuracy of positive AS-PATHs is about 99.5%, and the accuracy of Type-1 path hijacking is 87.5%.

TABLE III: Result of crafted AS-PATHs

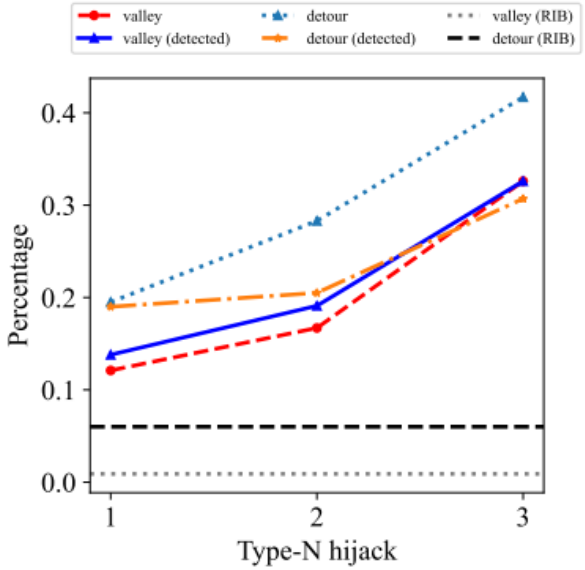
Type of AS-PATH	Number	Reliable link	Type-1 link	Type-2 link	valid AS-PATH	Suspicious AS-PATH				Accuracy
						Type-1	high	medium	low	
GREEN AS-PATHs	7000	11181	358	187	6966	5	3	6	**20**	**99.5%**
Type-1 Misconfiguration	1000	2231	108	985	167	0	924	0	0	92.4%
Type-2 Misconfiguration	1000	2174	496	582	256	247	528	0	0	77.5%
Type-1 hijacking	1000	2213	163	940	125	3	345	481	46	**87.5%**
Type-2 hijacking	1000	3018	153	984	493	2	322	176	7	50.7 %
Type-3 hijacking	1000	3706	160	935	700	0	250	50	0	30.0%
Type-1 BGP poisoning	1000	2237	236	940	107	14	879	0	0	89.3%
Type-2 BGP poisoning	1000	2241	372	2731	11	15	974	0	0	98.9%

Evaluation

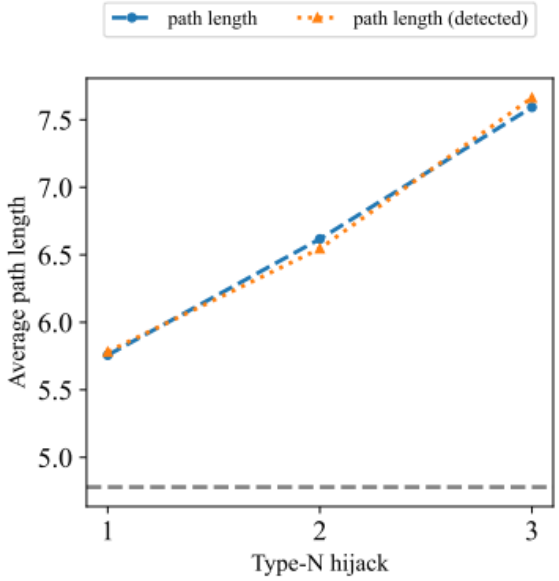
- Type-N hijacking： N is the **length of fake segment** in the AS-PATH.
- Normal AS-PATH:
  - 24514 24490 24489 23911 4538
- AS4538(CERNET) is attempt to hijack AS16509(AMAZON)
- Type-1 hijacking:
  - 24514 24490 24489 23911 4538 16509
  - Fake link : 4538-16059
- Type-2 hijacking:
  - 24514 24490 24489 23911 4538 3356 16509
  - Fake link : 4538-3356

Evaluation

- Type-N hijacking： N is the **length of fake segment** in the AS-PATH.
- Path hijacking
  - AS the N grows, the fake AS-PATHs will more likely to cause valley, traffic detour and longer AS-PATH.



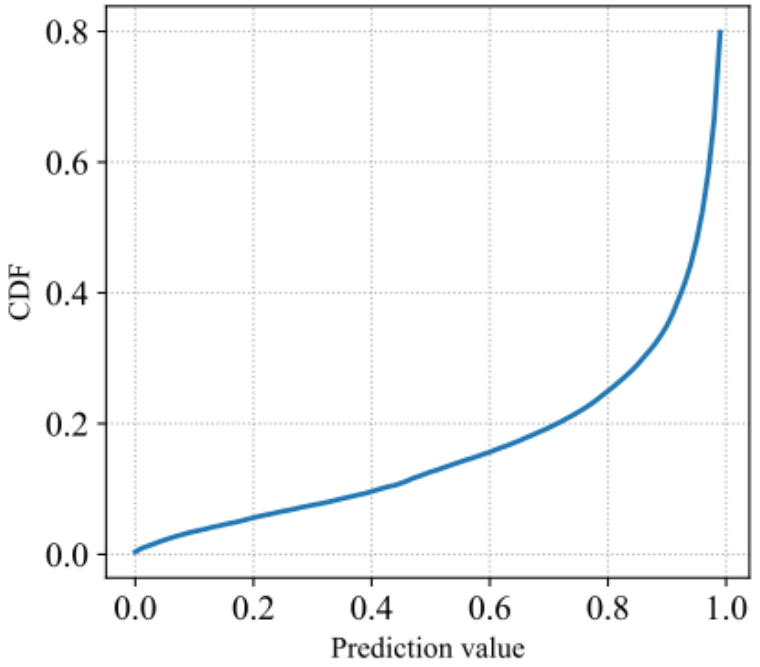
(c)



(d)

Evaluation

- Argus vs Metis
  - Detection of BGP updates from RRC00 for the entire month of November 2021
  - Link prediction threshold set to 0.8， Metis filters 1255.2 unseen links, or 80.2% of all links.



Seen reliable link	New AS	Type-1 link	Suspicious Type-1 link	Type-2 link	Suspicious Type-2 link
161808.2	30	244	7.3	1321.0	302.5

Evaluation

- Historical path hijacking detection
- 7 of 18 detected
- false negative reason:
  - 1. some hijackings (bitcanal, etc.) insert ASNs registered in the RIR but not used, thus bypassing Metis' Type-1 detection.
  - 2. Some hijackings insert real unseen links.

Event title	Hijack type	Type-1 link Number	Type-2 link Number	(sub)MOAS	Origin AS set Format	Alarm
bitcanal_3	subprefix	1	0	✓	{V,N}	✗
bitcanal_4	subprefix	1	0	✓	{V,N}	✗
petersburg_unused_1	unused	1	0	✗	{N}	✗
petersburg_unused_2	unused	1	0	✗	{N}	✗
petersburg_1	subprefix	1	0	✓	{V,N}	✗
petersburg_2	subprefix	1	0	✓	{V,N}	✗
Torg_1	prefix	0	2	✓	{V,O}	✗
Torg_2	prefix	0	2	✓	{V,O}	✗
Torg_3	prefix	0	2	✓	{V,O}	✗
backconnect_3	subprefix	2	5	✓	{V,H,O}	✓
backconnect_5	subprefix	0	2	✓	{V,O}	✓
backconnect_6	subprefix	0	2	✓	{V,H,O}	✓
france_1	subprefix	0	1	✓	{V,O}	✓
enzu_1	subprefix	0	3	✗	{V}	✓
facebook_1	subprefix	0	2	✗	{V}	✗
calson_1	subprefix	1	0	✓	{V,O,N}	✓
Defcon_1	subprefix	0	1	✓	{V,H}	✗
amazon_1	prefix	0	1	✗	{V1,V2}	✓

Conclusion

- We have experimentally demonstrated that AS links are predictable.

- We proposed link prediction based fake AS-PATHs detection framework Metis. It can effectively detect fake AS-PATHs caused by misconfiguration, BGP poisoning and path hijacking and can save 80.2% data-plane cost for unseen link based system like Argus.
- Future work: link prediction values and AS-PATH features into an ML model to classify them automatically.

Thank You

Q&A