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.
Origin Hijacking

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

Prediction value > threshold

Type-2 link → Link predictor → ?

yes → valid

no → Type-2 rules

Suspicious, confidence score
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%.
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

<table>
<thead>
<tr>
<th>Type of AS-PATH</th>
<th>Number</th>
<th>Reliable link</th>
<th>Type-1 link</th>
<th>Type-2 link</th>
<th>valid AS-PATH</th>
<th>Suspicious Type-1</th>
<th>AS-PATH</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>GREEN AS-PATHs</td>
<td>7000</td>
<td>11181</td>
<td>358</td>
<td>187</td>
<td>6966</td>
<td>5</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Type-1 Misconfiguration</td>
<td>1000</td>
<td>2231</td>
<td>108</td>
<td>985</td>
<td>167</td>
<td>0</td>
<td>924</td>
<td>0</td>
</tr>
<tr>
<td>Type-2 Misconfiguration</td>
<td>1000</td>
<td>2174</td>
<td>496</td>
<td>582</td>
<td>256</td>
<td>247</td>
<td>528</td>
<td>0</td>
</tr>
<tr>
<td>Type-1 hijacking</td>
<td>1000</td>
<td>2213</td>
<td>163</td>
<td>940</td>
<td>125</td>
<td>3</td>
<td>345</td>
<td>481</td>
</tr>
<tr>
<td>Type-2 hijacking</td>
<td>1000</td>
<td>3018</td>
<td>153</td>
<td>984</td>
<td>493</td>
<td>2</td>
<td>322</td>
<td>176</td>
</tr>
<tr>
<td>Type-3 hijacking</td>
<td>1000</td>
<td>3706</td>
<td>160</td>
<td>935</td>
<td>700</td>
<td>0</td>
<td>250</td>
<td>50</td>
</tr>
<tr>
<td>Type-1 BGP poisoning</td>
<td>1000</td>
<td>2237</td>
<td>236</td>
<td>940</td>
<td>107</td>
<td>14</td>
<td>879</td>
<td>0</td>
</tr>
<tr>
<td>Type-2 BGP poisoning</td>
<td>1000</td>
<td>2241</td>
<td>372</td>
<td>2731</td>
<td>11</td>
<td>15</td>
<td>974</td>
<td>0</td>
</tr>
</tbody>
</table>
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.
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.

<table>
<thead>
<tr>
<th>Seen reliable link</th>
<th>New AS</th>
<th>Type-1 link</th>
<th>Suspicious Type-1 link</th>
<th>Type-2 link</th>
<th>Suspicious Type-2 link</th>
</tr>
</thead>
<tbody>
<tr>
<td>161808.2</td>
<td>30</td>
<td>244</td>
<td>7.3</td>
<td>1321.0</td>
<td>302.5</td>
</tr>
</tbody>
</table>
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.
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