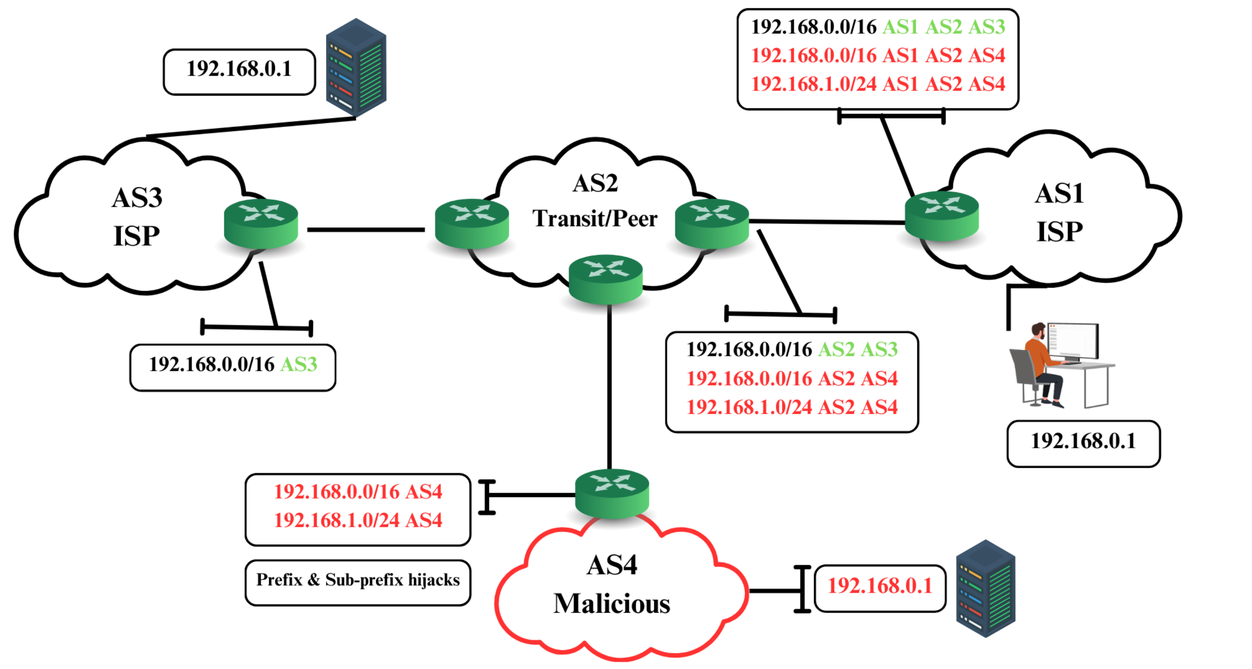
Quantifying the Proportion of Hijacked Prefixes Among the Identified Prefix Hijackers

Ebrima Jaw†, Moritz Müller†*, Cristian Hesselman†*, Lambert Nieuwenhuis†
†University of Twente, Enschede, *SIDN Labs, Arnhem, The Netherlands

1 BGP: Overview

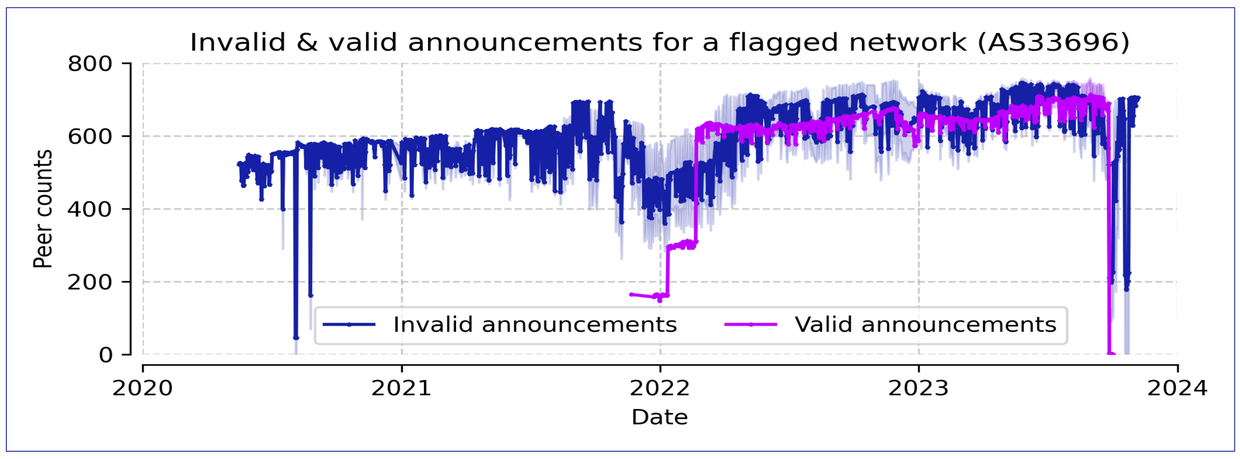
- **The Border Gateway Protocol (BGP)** is the Internet's default routing protocol that enables the **exchange of reachability information** among **Autonomous Systems (ASes)**.
- However, **BGP** is vulnerable to **prefix origin hijacks**.
  - **Prefix origin hijacks** are ***malicious*** or ***unintentional announcements*** of IP prefixes that belong to other ASes.
- "***Serial hijacker(s)"*** are ***ASes*** that ***repeatedly*** hijack other prefixes for ***months*** or ***years***.

2 BGP: Operations & Security Issues



3 Motivation and Research Goal

- The motive for **serial hijacking** remains unknown.
- Surprisingly, we observed **higher visibility** for RPKI-invalid hijacked prefixes
- Our study aims to better understand the magnitude of **serial hijacking events** and their **motives**.



4 Methodology

- Use **RPKI daily snapshots** to determine the **level of RPKI protections** against our flagged ASes.
- Filter **RPKI-invalid announcements** for our ***flagged Ases. Used AS mapping*** to determine **victim networks**.
- Use **ASRank** and **AS relationship** dataset to determine any possible relationship between hijackers and victims.

5 RPKI-invalid Announcements

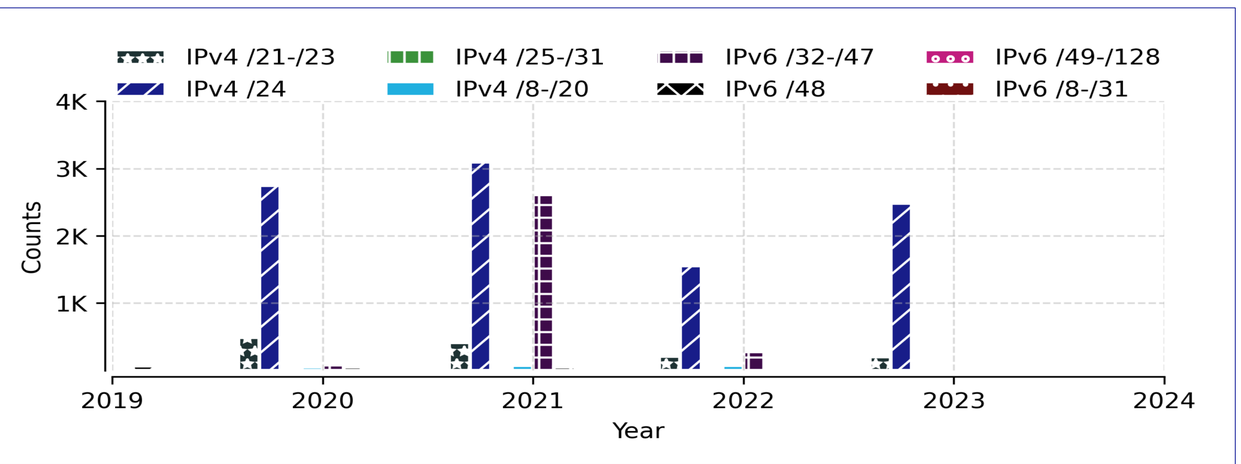
Year	Invalids	Invalid length	Unknown	Valid
2020	**3.4K (36%)**	1.6K (16%)	3.6K (37%)	**1.0K (11%)**
2023	**2.8K (10%)**	3.7k (13%)	6.5K (23%)	**15K (54%)**

- **Observations**: Decrease in the no. of ***invalid announcements*** over time. (***Potentially due to ROV***)
- Large no. of ***upstream providers*** not enforcing **ROV.**

RIPE	ARIN	APNIC	AFRINIC	LACNIC
8K (44%)	**6K (31%)**	2K (11%)	1K (8%)	933 (5%)
Announcement share of unallocated prefixes				
1K (15%)	**2K (43%)**	296 (15%)	123 (9%)	**284 (30.4%)**

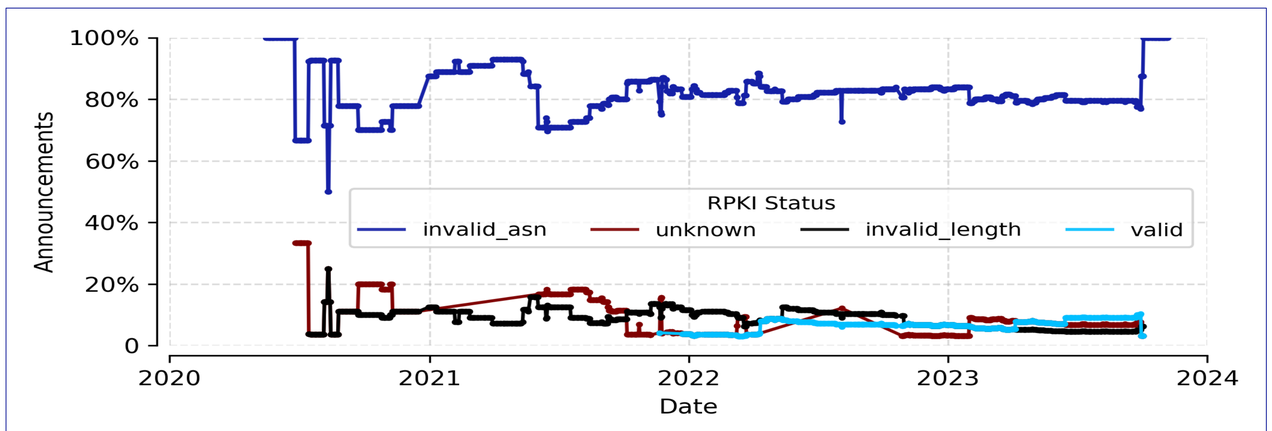
- **Observations**: **RIPENCC** and **ARIN** resources (prefixes) are more likely to be hijacked than other RIR.

6 Common Hijacked Prefix Lengths



- **Observations**: Hijacked invalid prefixes are mainly /24 .

7 Results: A Serial Hijacking Case Study



- **Observations**: Avg. of **82%** invalid announcements
- Announced prefixes of **64** different ASes in **5 regions**.