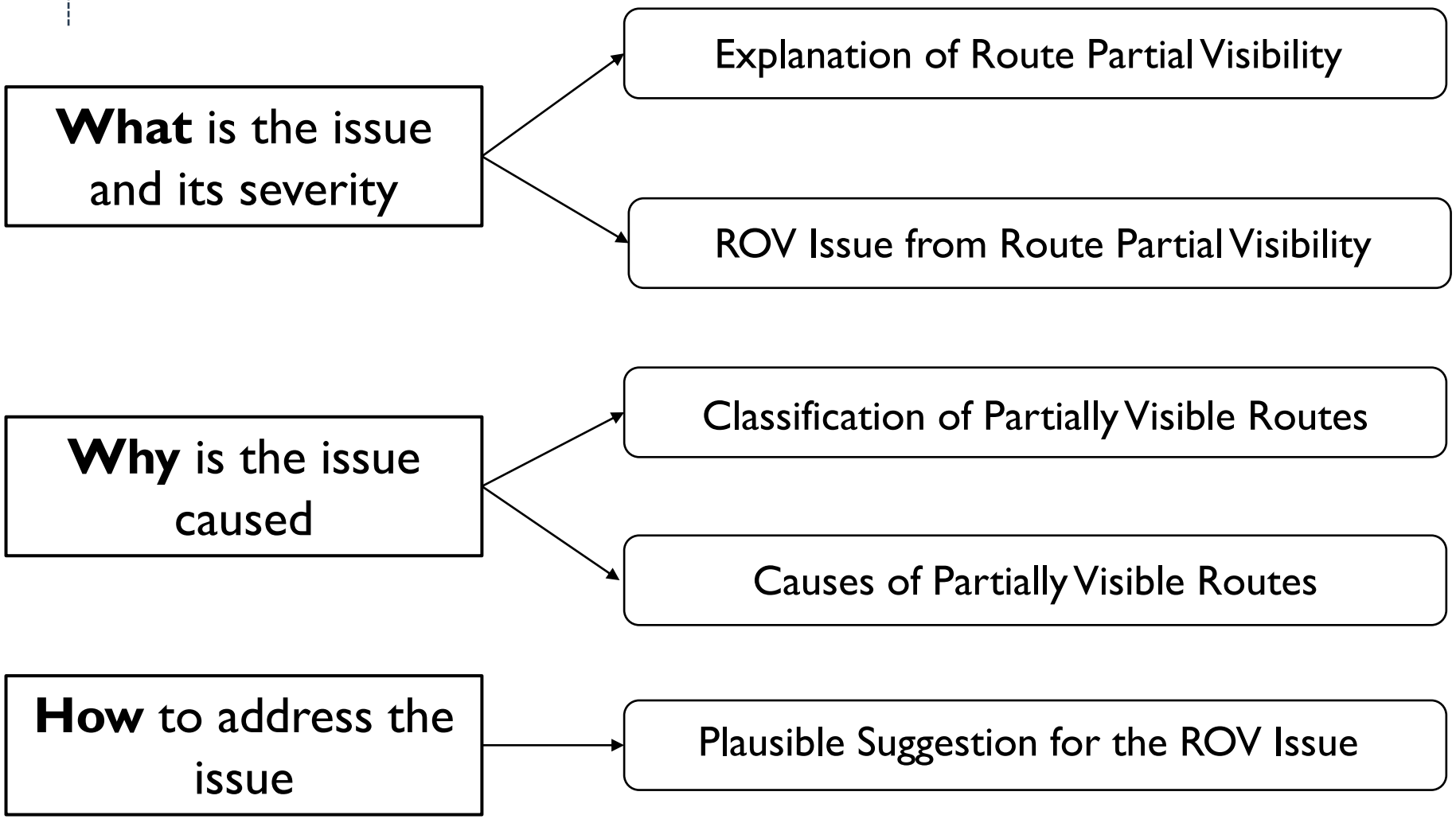
Issue in Route Origin Validation (ROV) from Route Partial Visibility

Beijing Zhongguancun Lab, Tsinghua University

Shuhe Wang, Ke Xu, Qi Li, Zhuotao Liu

2024.11.05

Content


What is the issue and its severity
Explanation of Route Partial Visibility
ROV Issue from Route Partial Visibility
Why is the issue caused
Classification of Partially Visible Routes
Causes of Partially Visible Routes
How to address the issue
Plausible Suggestion for the ROV Issue

Explanation of Route Partial Visibility

Definition: a route that is *visible to all* ASes is defined as a *fully visible route*, otherwise it is called a *partially visible route*

Example cases

Received routes:
- 1.0.1.0/24, AS 1
- 1.0.2.0/23, AS 2

AS 100

Received routes:
- 1.0.1.0/24, AS 1
- 1.0.3.0/24, AS 2

AS 200

Received routes:
- 1.0.1.0/24, AS 1
- 1.0.4.0/24, AS 3

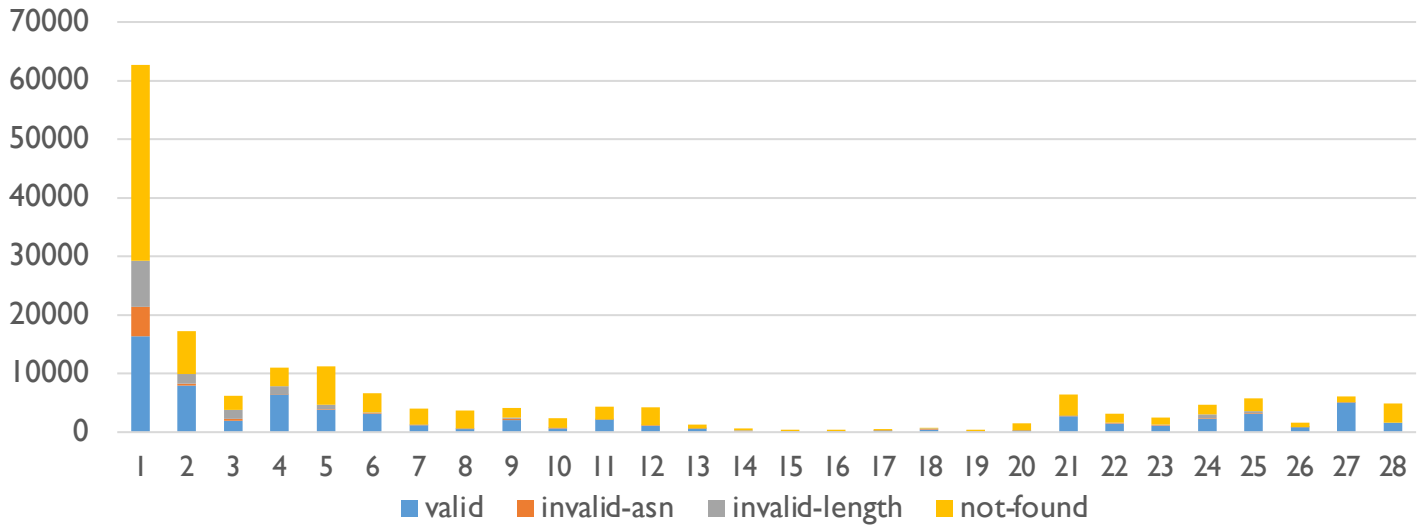
AS 300

Fully visible routes
- 1.0.1.0/24, AS 1

Partially visible routes
- 1.0.2.0/23, AS 2
- 1.0.3.0/24, AS 2
- 1.0.4.0/24, AS 3

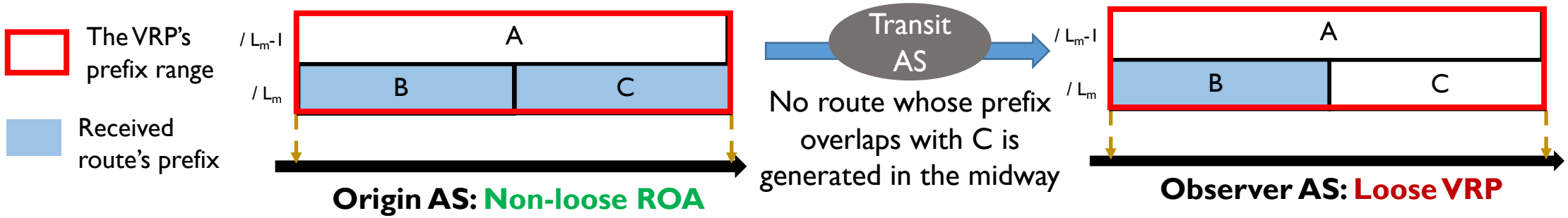
- Setting of route visibility observation experiment
  - 28 *feasible* (means > 900000 advertised IPv4 routes are received) vantage points (VPs)
  - 27 Route Views VPs across all 5 RIRs + 1 CERNET VP (located in Beijing)

- Number & ROV states of partially visible routes on each VP



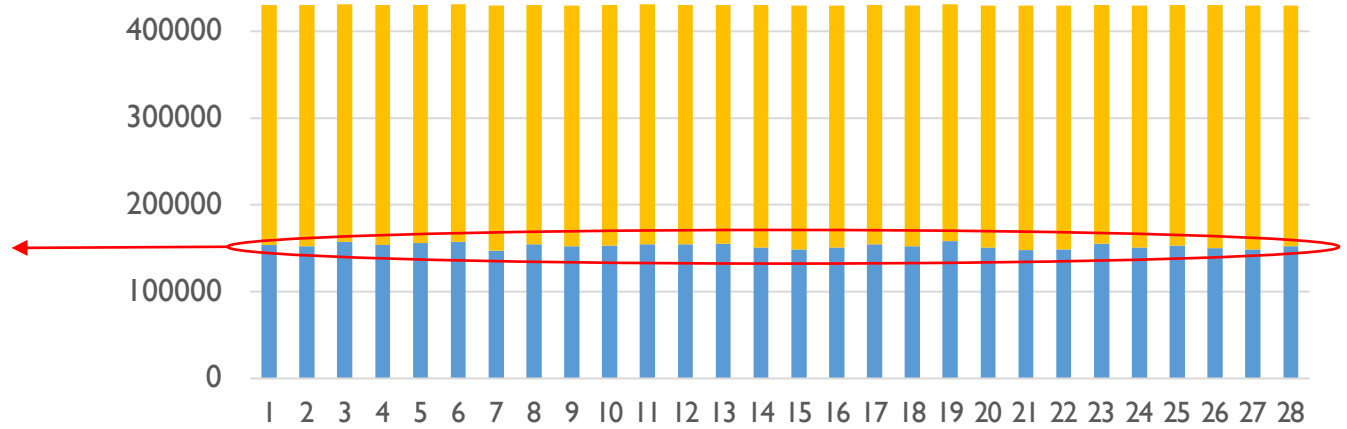
ROV Issue from Route Partial Visibility

Issue: the VRP could be "loose"[1], since routes of *all* sub-prefixes of the maximum length allowed by whom are not *totally* received



- VRP looseness on each VP

Loose VRP at each VP is around 36%, While currently loose ROA is far less then 10%

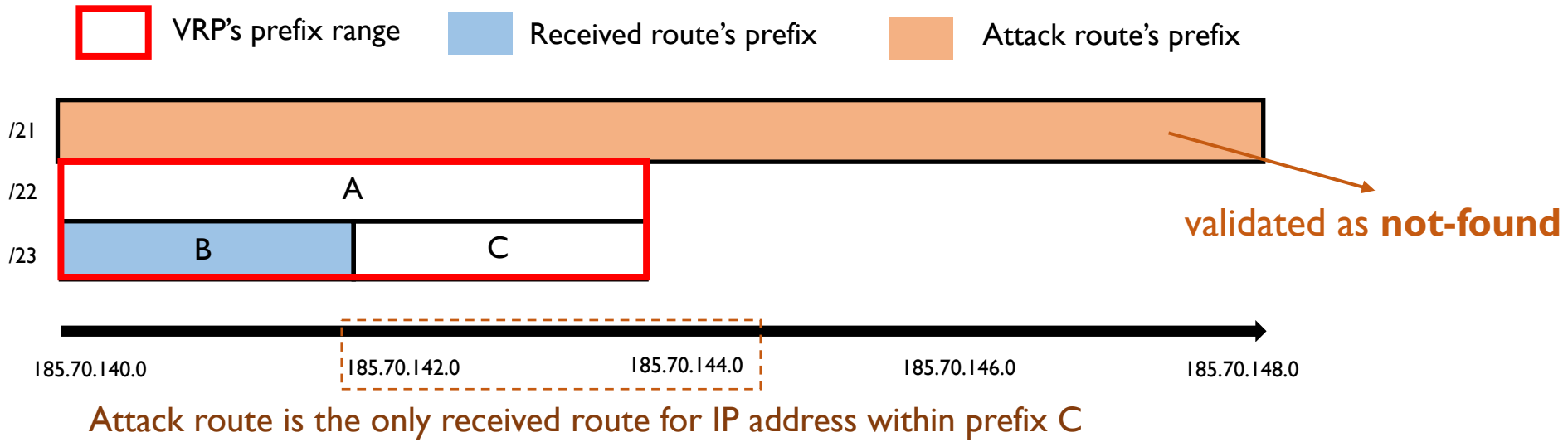


Note [1]: The concept of "loose" is first raised by the paper "Are we there yet? On RPKI's deployment and security" in 2016. The concept is also used in RFC 9319 "The Use of maxLength in RPKI".

ROV Issue from Route Partial Visibility

Vulnerabilities of loose VRPs:

- Super-prefix hijack[1]
- Forged-origin hijack

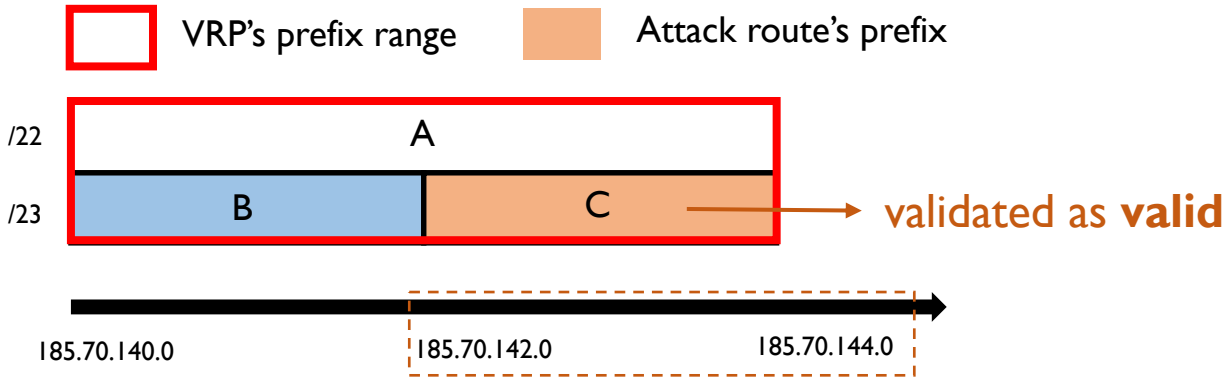


Note [1]: Super-prefix hijack is also described and discussed in previous work: "ROV++: Improved Deployable Defense against BGP Hijacking" in NDSS 2021.

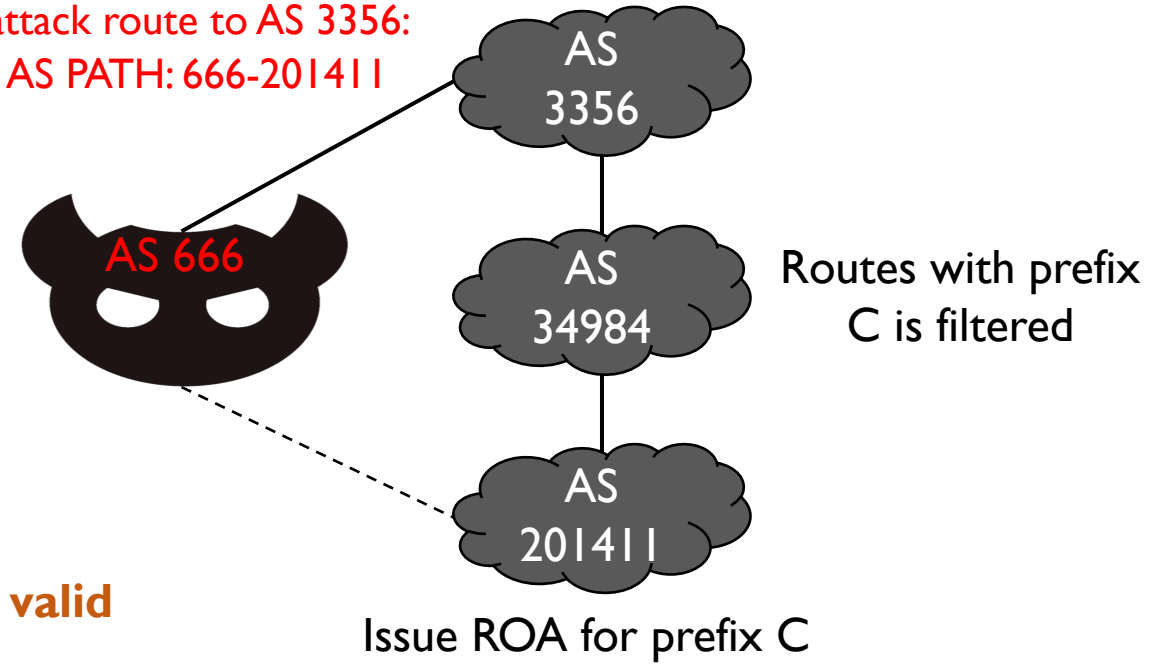
ROV Issue from Route Partial Visibility

Vulnerabilities of loose VRPs :

- Super-prefix hijack
- Forged-origin hijack[1]



Attack route is the only received route for IP address within prefix C



Note [1]: A detailed description and discussion of forged-origin hijacks are presented in RFC 9319 "The Use of maxLength in RPKI".

Classification of Partially Visible Routes

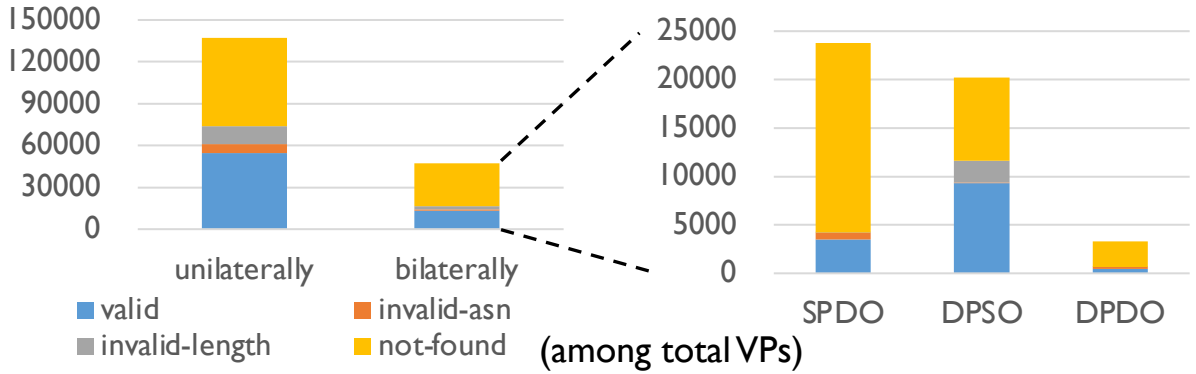
1. Unilaterally (partially) visible route

- There exist some ASes receiving no route whose prefix overlaps with such route's prefix.

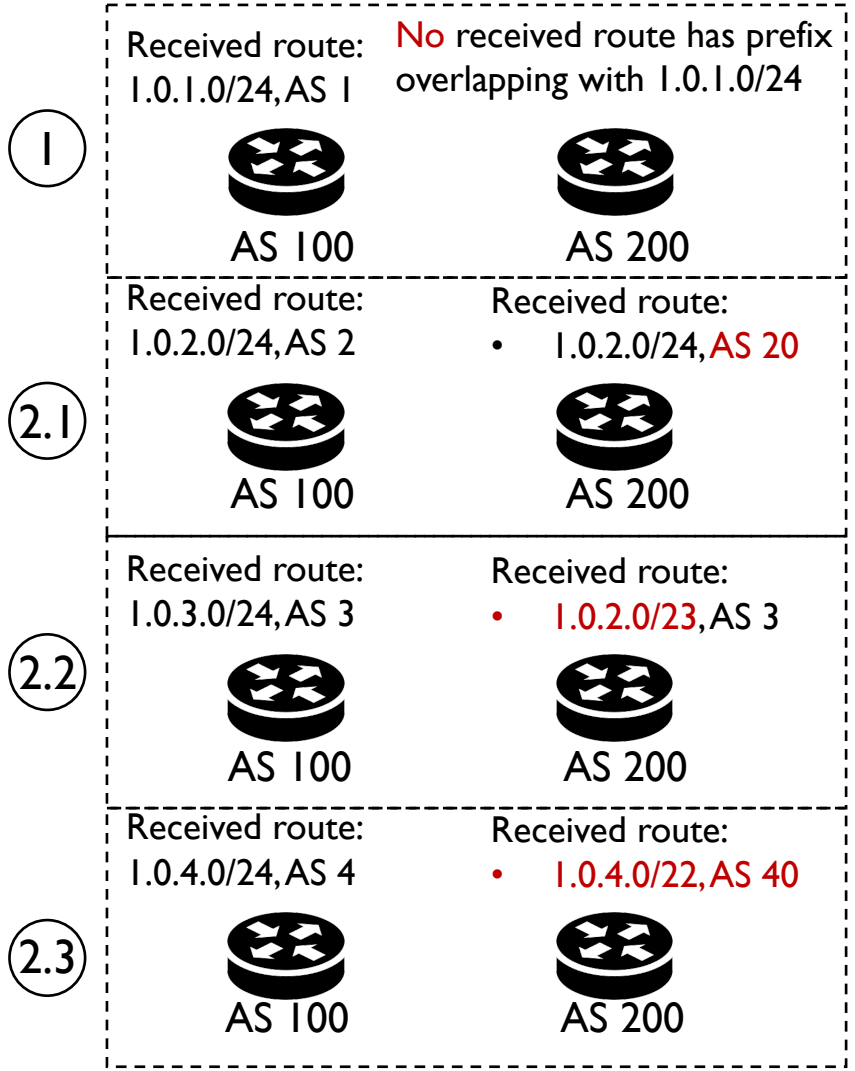
2. Bilaterally (partially) visible route

- There exist some ASes receiving certain route whose prefix overlaps with such route's prefix (such pair of routes is called a *conjugate route pair*).
- Further classification of *conjugate route pair:*
  - **2.1 SPDO:** the same prefix, but different origin ASes.
  - **2.2 DPSO:** different prefixes, but the same origin AS.
  - **2.3 DPDO:** both origin ASes and prefixes are different.

- Numbers & ROV states of each type of partially visible routes

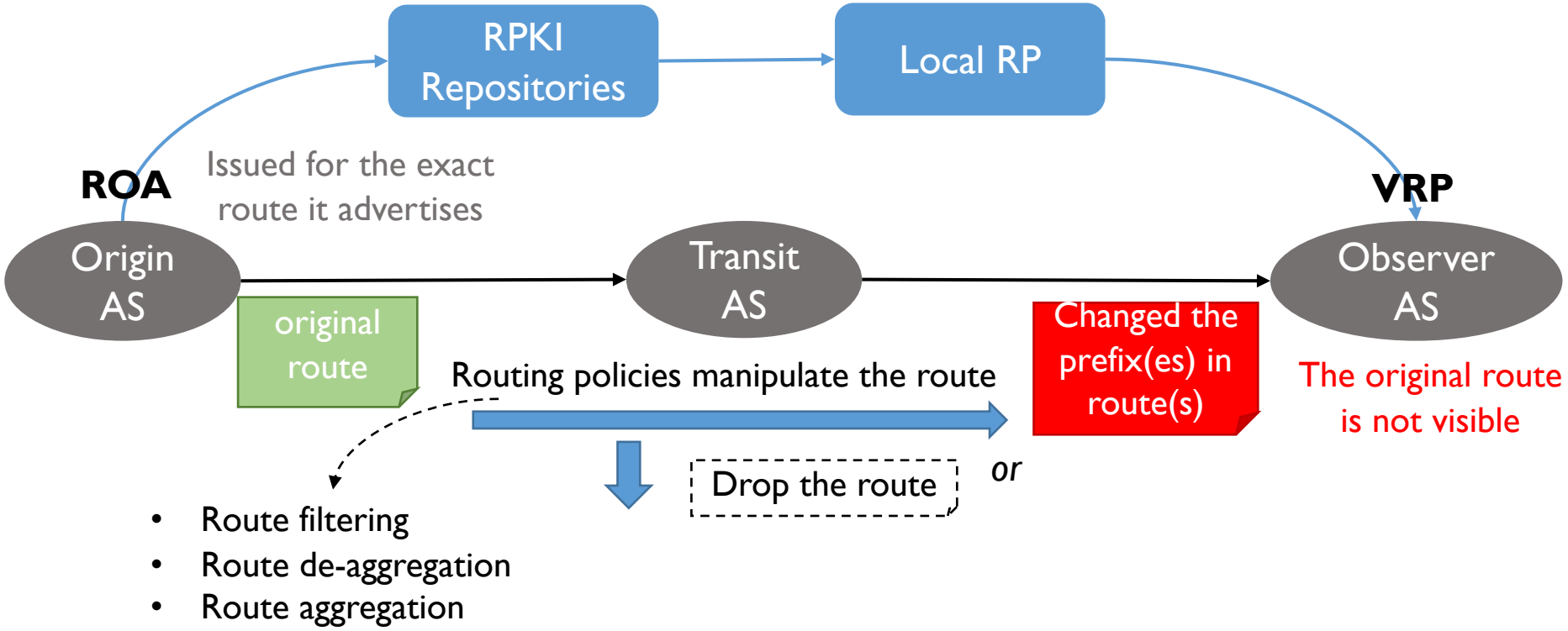


(among total VPs)



Causes of Partially Visible Routes

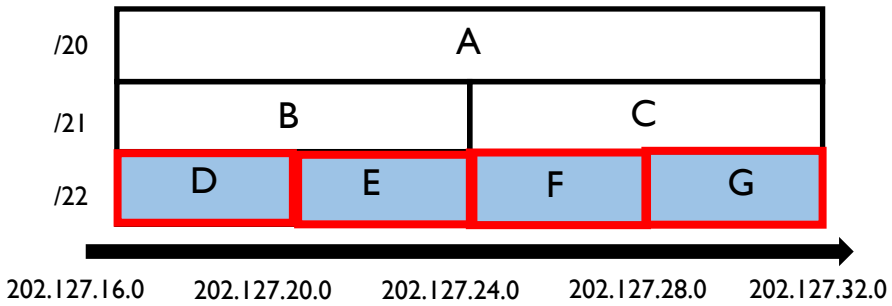
- **Formation of Route Partial Visibility**
  - different routing policies in transit AS (we call such policies as ***policies with hidden danger***) could cause different types of partially visible routes



Causes of Partially Visible Routes

Cause 1: route filtering in transit AS

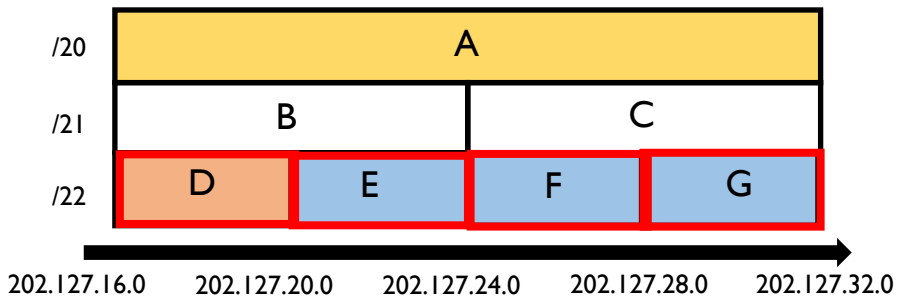
- Effect
  - *Unilaterally visible routes*, and
  - *SPDO* pairs of bilaterally visible routes if *MOAS* prefixes exist
- Typical policies:
  - Import / Export filtering
  - Route blackhole
  - Route damping



VRPs' prefix ranges

- VRP 1: AS 1, 202.127.16.0/22-22 (D)
- VRP 2: AS 2, 202.127.16.0/22-22 (E)
- VRP 3: AS 3, 202.127.24.0/22-22 (F)
- VRP 4: AS 4, 202.127.28.0/22-22 (G)

Filter out D



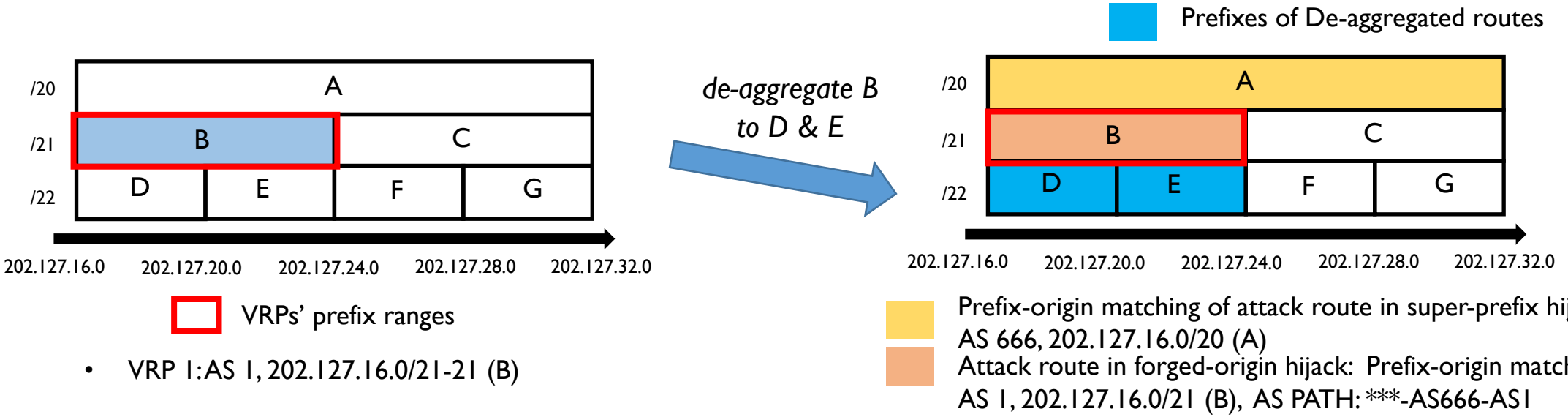
Prefix-origin matching of attack route in super-prefix hijack: AS 666, 202.127.16.0/20 (A)

Attack route in forged-origin hijack: Prefix-origin matching: AS 1, 202.127.16.0/22 (D), AS PATH: ***-AS666-AS1

Causes of Partially Visible Routes

Cause 2: route de-aggregation in transit AS

- Description
  - Route de-aggregation will *suppress* the original route, and generate one or a few routes whose prefixes are the sub-prefixes of the original prefix, while the origin AS is *unchanged*
- Effect
  - *DPSO* pairs of bilaterally visible routes

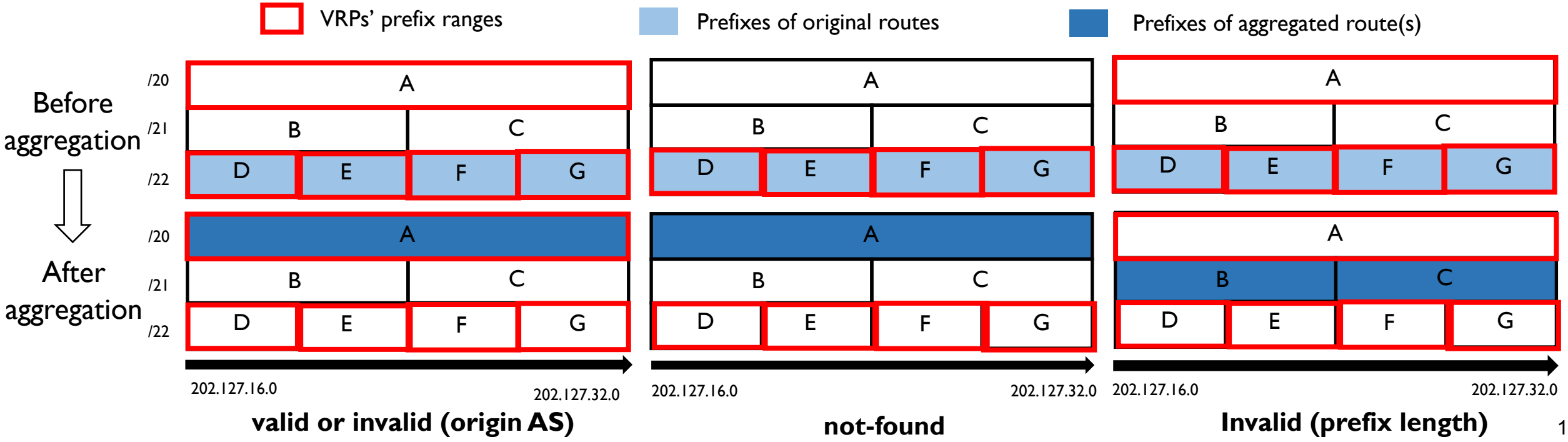


- VRP 1: AS 1, 202.127.16.0/21-21 (B)

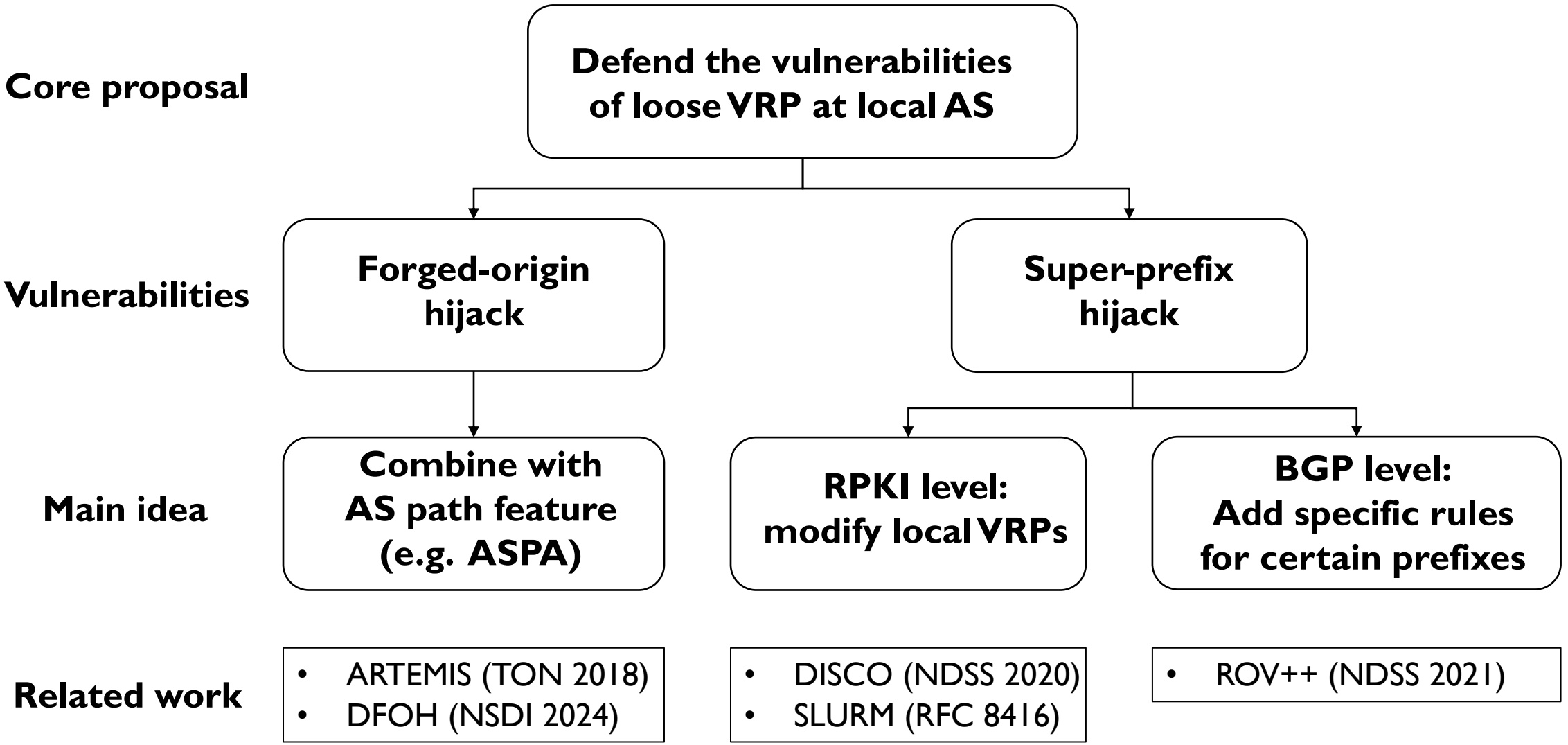
Causes of Partially Visible Routes

Cause 3: route aggregation in transit AS

- Description
  - Route aggregation will *suppress* the original routes, and generate an aggregated route whose prefix is the *super-prefix* of all original prefixes
- Effect
  - *DPSO / DPDO pairs of bilaterally visible routes* depending on if *the AS doing aggregation = the origin AS*
  - The ROV state of the aggregated route could be valid, not-found or invalid.



Plausible Suggestion for the ROV Issue



Conclusions

- **Route partial visibility** could cause VRP to become **loose**, thus will be vulnerable to route hijacking including *super-prefix hijack* and *forged-origin hijack*.

- There are multiple types of partially visible routes, each of which are possibly caused by a unique type of *routing policy with hidden danger* in transit AS, including *route filtering*, *route de-aggregation* and *route aggregation*.

- To mitigate such issue, a plausible suggestion is trying to *defend the vulnerabilities of loose VRPs at each AS locally*.

Thank you!

Welcome to discuss with me at wangsh@mail.zgclab.edu.cn