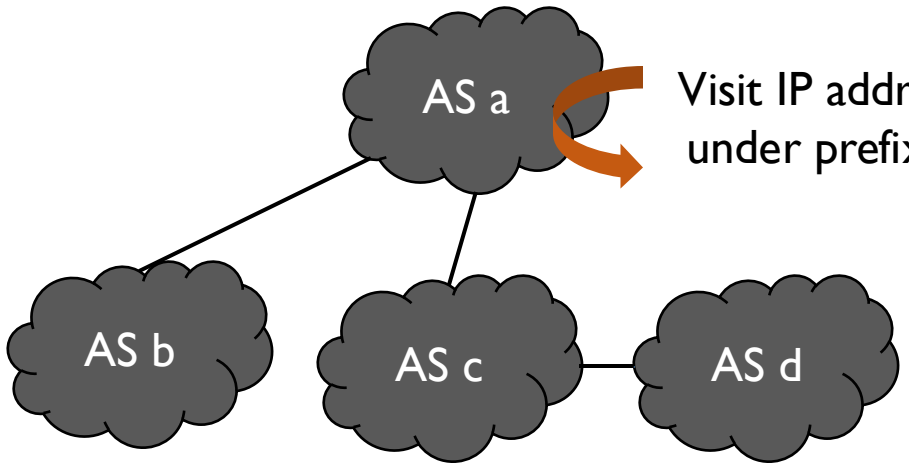
The Inconsistency Issue between the Looseness of ROAs and VRPs

Beijing Zhongguancun Lab, Tsinghua University

Shuhe Wang, Ke Xu, Qi Li, Zhuotao Liu, Xingang Shi, Hui Wang, Xiaoliang Wang

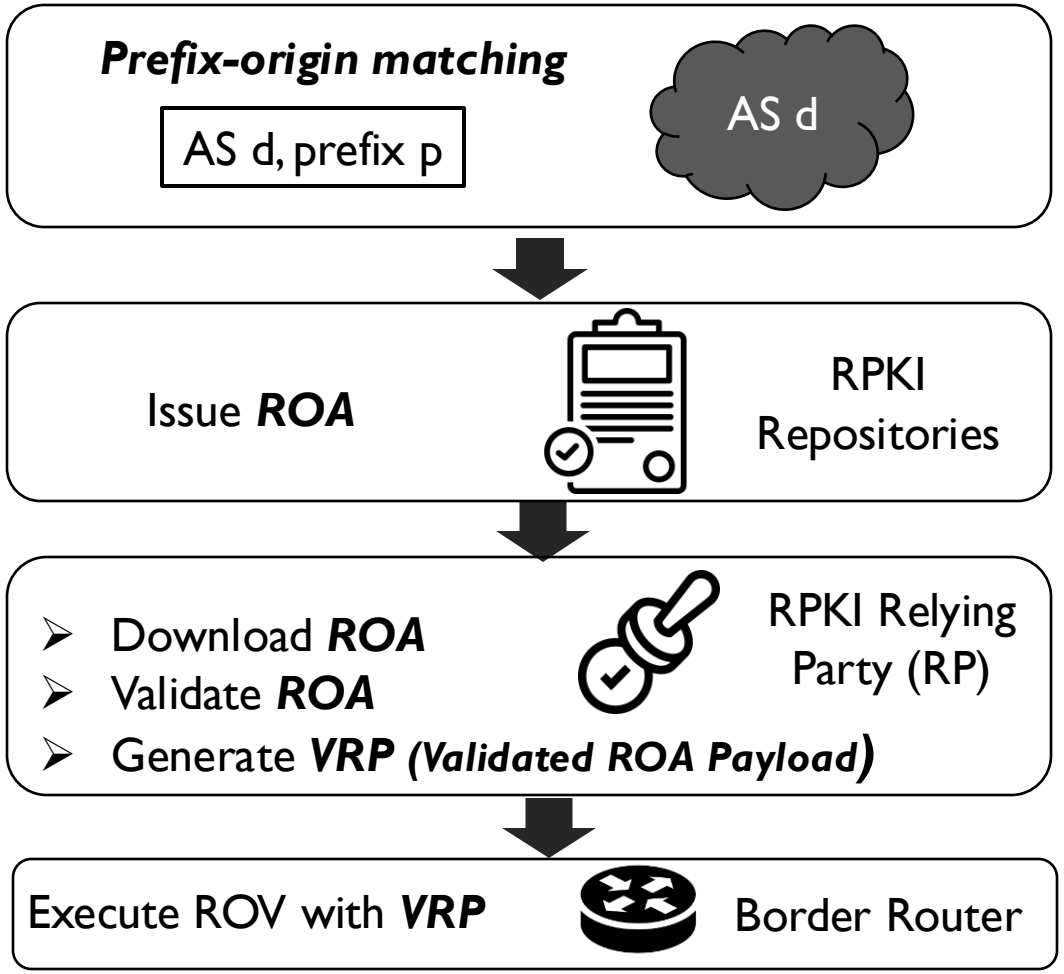
BGP and RPKI

BGP: vulnerable to route hijacking



AS path a-b is shorter than a-c-d: AS b is able to hijack prefix p

RPKI: validate the prefix-origin matching



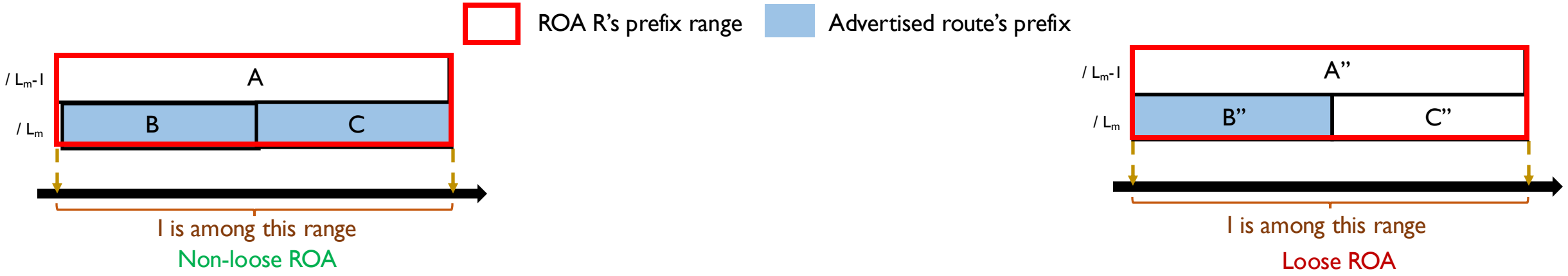
Content

Q1: ***What*** is the looseness of ROAs & VRPs[1]?

Note [1]: The ROAs and their corresponding VRPs are all **active** in our discussion, which means neither they or part of them are *expired or revoked*, otherwise they may have security issues according to to [draft-li-sidrops-roa-granularity-problem]

Definition of loose ROAs

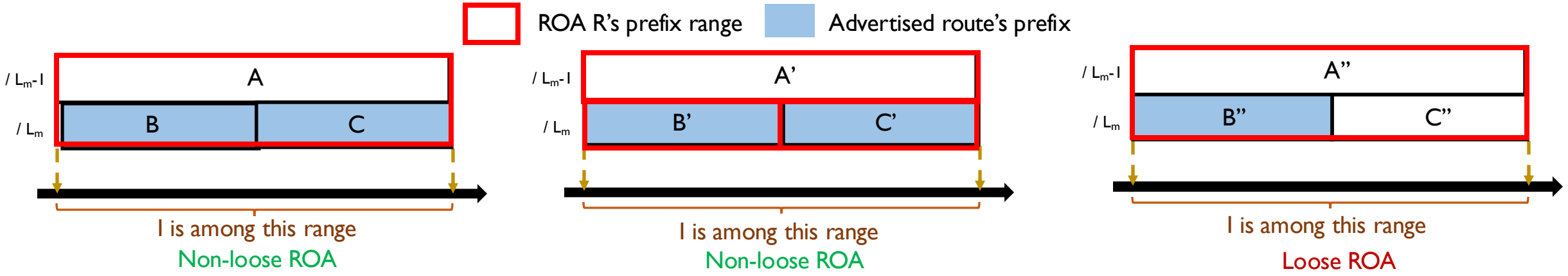
- **Previous definition of loose[1] ROAs:** *not all* sub-prefixes of the maximum length allowed by whom are advertised in BGP



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".

Definition of loose ROAs

- **Previous definition of loose[1] ROAs:** *not all* sub-prefixes of the maximum length allowed by whom are advertised in BGP
- **Renewed definition of loose ROAs:** an ROA R that *fails to satisfy* the following restrictions:
  - For any IP address I covered by R, there always exists an *advertised route:*
    - Whose prefix p covers I
    - Which is validated as *valid* (not necessarily validated by R)
    - Whose prefix length L is the longest among all advertised routes whose prefixes cover I
    - Whose prefix length $L \geq L_m$, where L_m is R's MaxLength

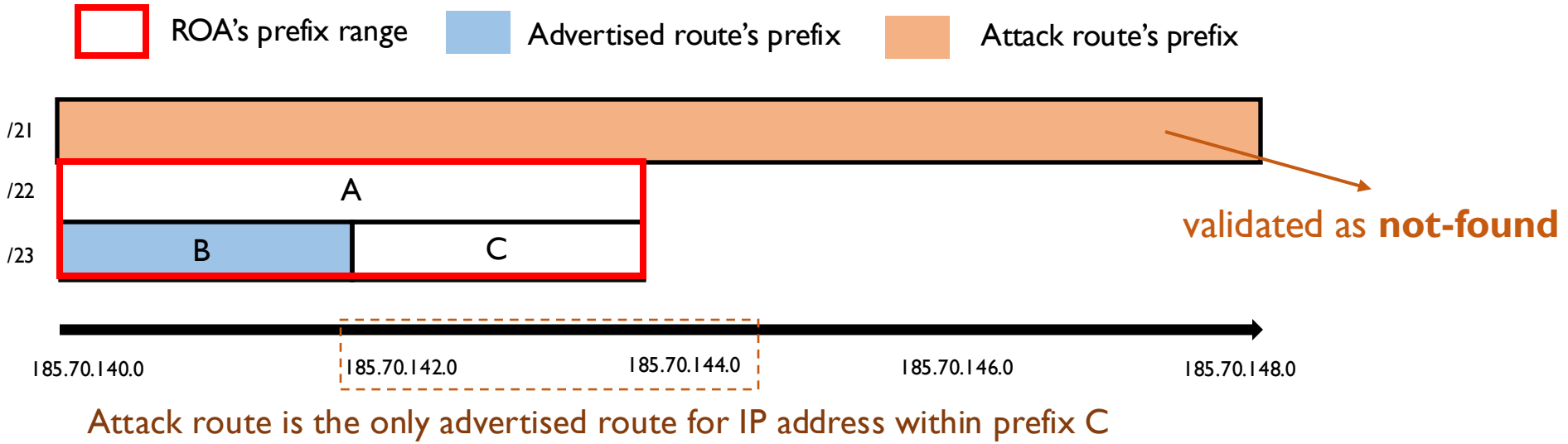


Note [1]: The concept of "loose" is first raised by the paper "Are we there yet? On RPKI's deployment and security" in 2016. The concept is also used in RFC 9319 "The Use of maxLength in RPKI".

Vulnerabilities of loose ROAs

Vulnerabilities:

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

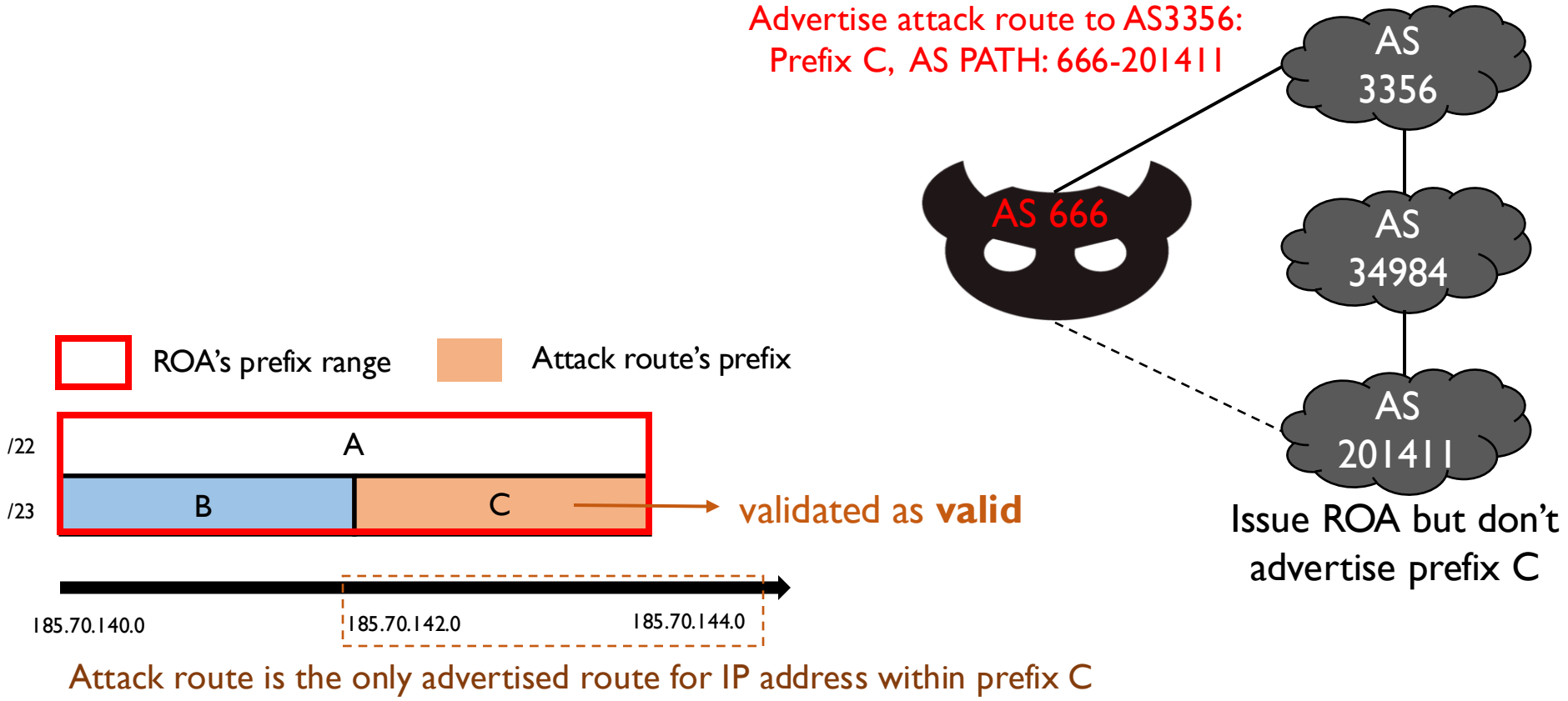


Note [1]: Super-prefix hijack is also described and discussed in previous work: "ROV++: Improved Deployable Defense against BGP Hijacking" in NDSS 2021.

Vulnerabilities of loose ROAs

Vulnerabilities:

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



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

Definition of loose VRPs

An *active* ROA R is loose if *fails to satisfy* the following restrictions:

- For any IP address I covered by R, there exists an *advertised route*:
  - Whose prefix p covers I
  - Which is validated as *valid* (not necessarily validated by R)
  - Whose prefix length L is the longest among all advertised routes whose prefixes cover I
  - Whose prefix length L $\geq L_m$, where L_m is R's MaxLength

Similar definitions

A VRP V on a router is loose if it *fails to satisfy* the following restrictions :

- For any IP address I covered by V, there exists a *route in the router's local RIB:*
  - Whose prefix p covers I
  - Which is validated as *valid* (not necessarily validated by V)
  - Whose prefix length L is the longest among all routes in the local RIB whose prefixes cover I
  - Whose prefix length L $\geq L_m$, where L_m is V's MaxLength

Content

Q2: ***Do*** ROAs & VRPs have consistent looseness?

Visions of prefix-origin matchings

- Answer to Q2: Sadly no, because an originally announced route may not be able to advertised to another observer AS
- Setting of observation of route visibility across the world
  - 28 *feasible* VPs (vantage point): feasible means each VP can collect most advertised IPv4 routes (> 900000)
  - 27 Route Views VPs across all 5 RIRs + 1 CERNET VP (located in Beijing)

Count of VPs	Total	APNIC	RIPE NCC	ARIN	LACNIC	AFRNIC
feasible	28	6 + 1	4	10	4	3

- We define the ***prefix-origin matching*** in a route that is *visible to all* VPs as ***fully visible matching***, otherwise it is called ***partially visible matching***

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

VP 1

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

VP 2

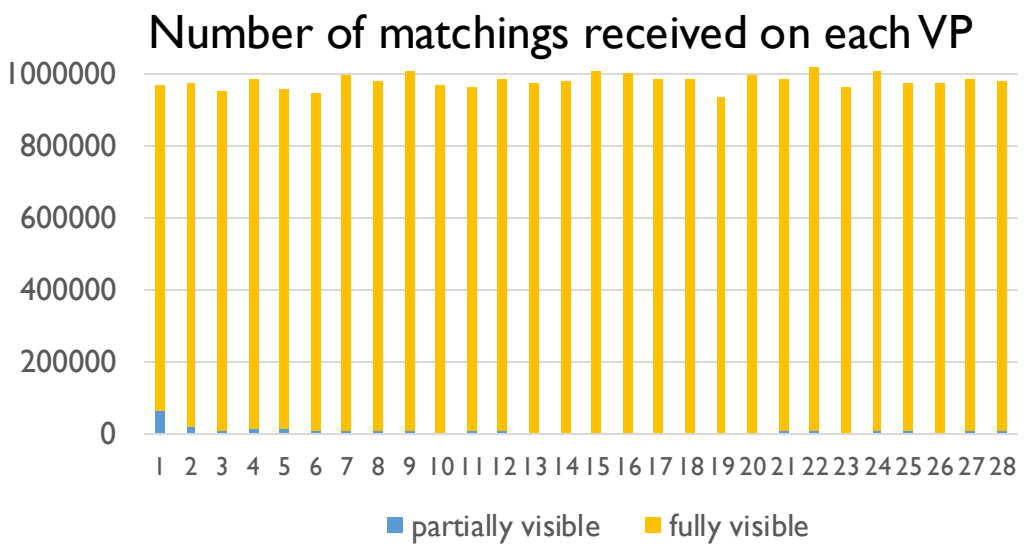
Received matchings:
- 1.0.1.0/24,AS 1
- 1.0.4.0/24,AS 3

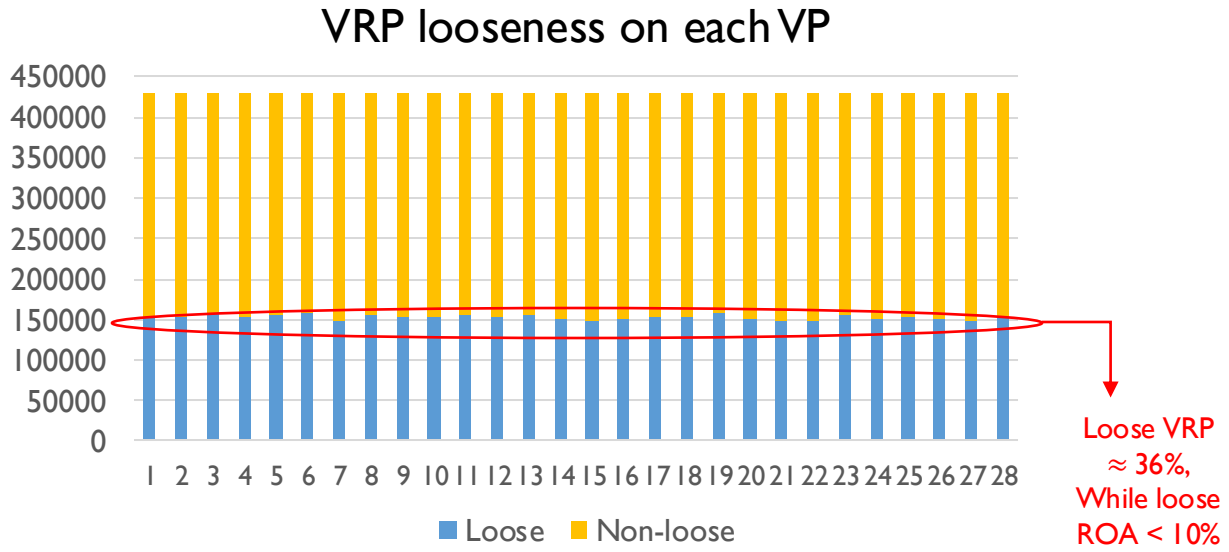
VP 3

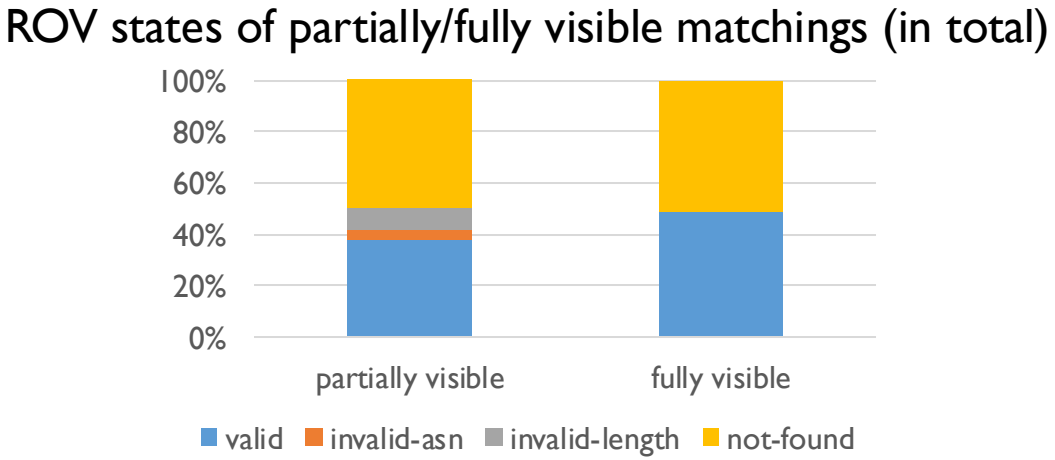
Fully visible matchings
- 1.0.1.0/24,AS 1

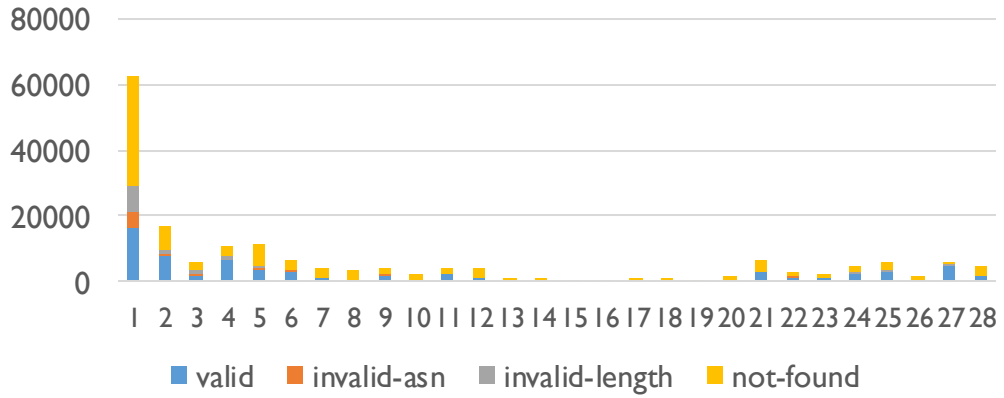
Partially visible matchings
- 1.0.2.0/23,AS 2
- 1.0.3.0/24,AS 2
- 1.0.4.0/24,AS 3

Visions of prefix-origin matchings









Observation 1: obviously diverse visions of prefix-origin matchings on different VPs

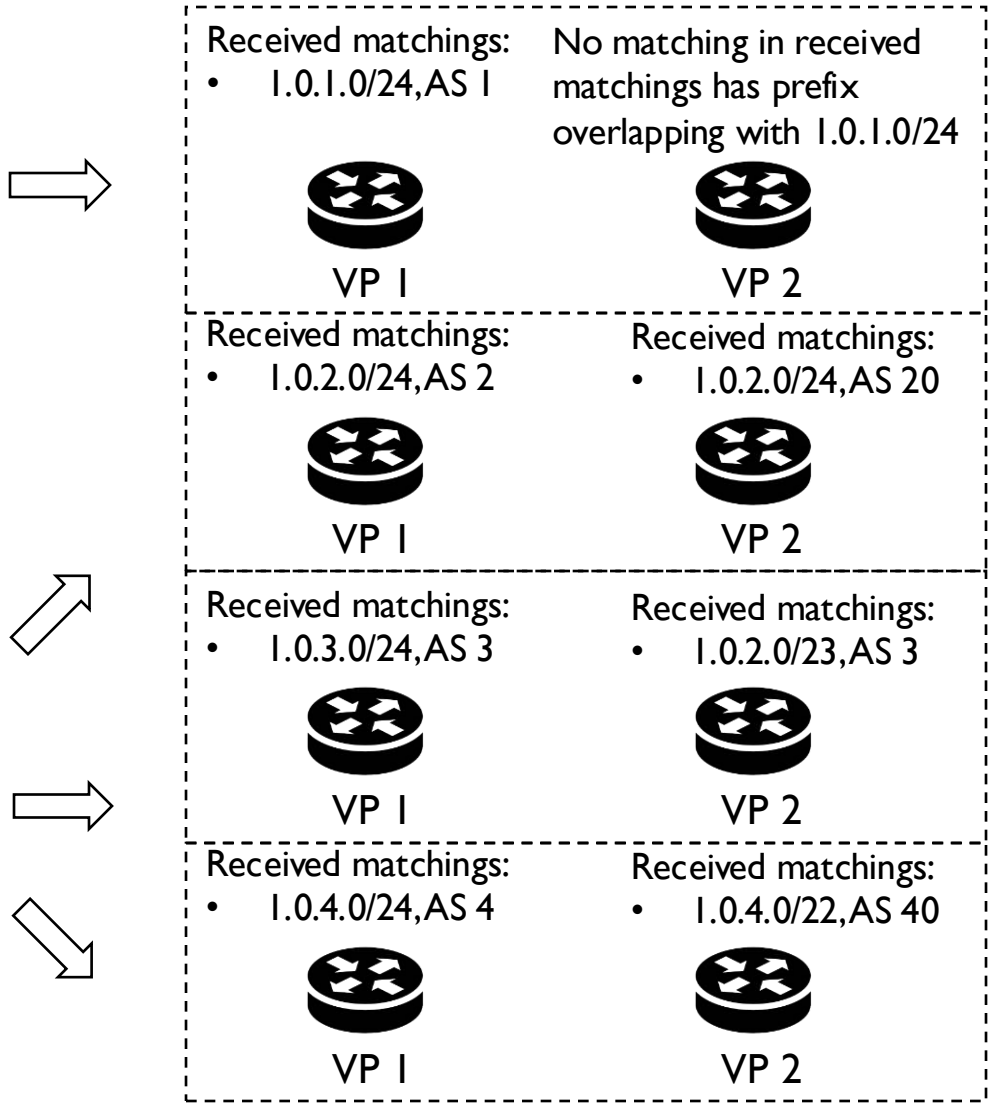
Classification of partially visible matchings

Unilaterally (partially) visible

- for a unilaterally visible Matching M, in those ASes where the matching is invisible, there is no matching whose prefix is overlapped with M's prefix.

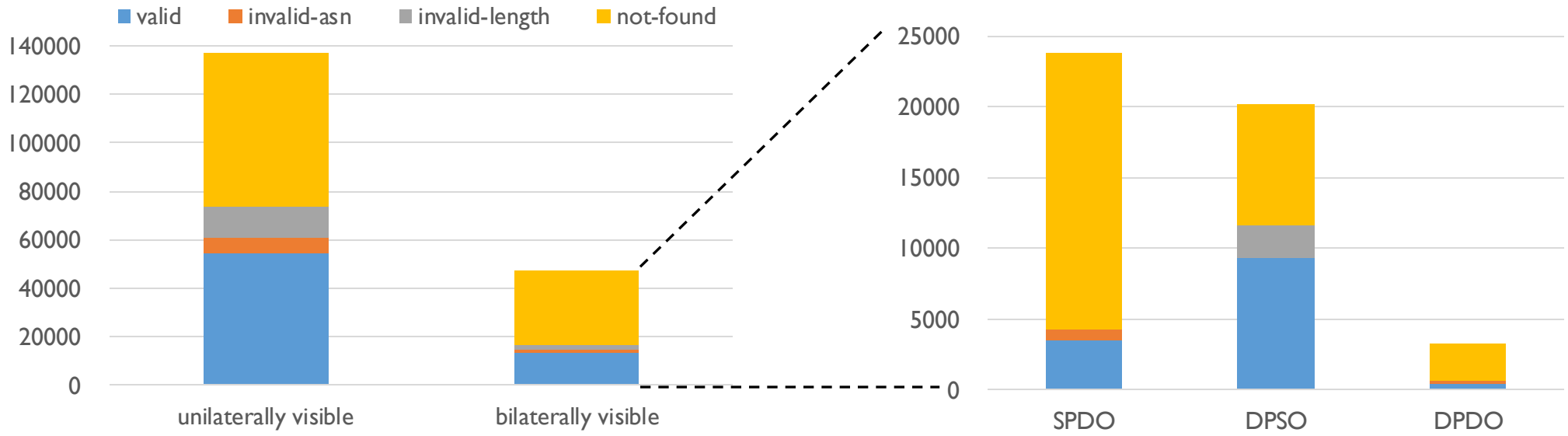
Bilaterally (partially) visible

- For a bilaterally visible route M, in those ASes where the matching is invisible, there exists another visible matching whose prefix is overlapped with M's prefix (These 2 matchings are called a *conjugate matching pair*).
- Further classification of *conjugate matching pair:*
  - **SPDO:** same prefix, different origin AS. SPDO matching pair is the result of MOAS prefixes.
  - **DPSO:** different prefix, same origin AS.
  - **DPDO:** both origin AS and prefixes are different.



Classification of partially visible matchings

Numbers and ROV states of unilaterally/bilaterally visible matchings (in total)



ROV states of conjugate DPSO pairs

shorter prefix \ longer prefix	valid	Invalid ASN	Invalid length
Valid	-	0	1807
Invalid-asn	8	-	20
Invalid-length	37	0	-
Not-found	51	8	6

ROV states of conjugate DPDO pairs

shorter prefix \ longer prefix	valid	Invalid ASN	Invalid length
Valid	-	205	90
Invalid-asn	189	-	9
Invalid-length	1	0	-
Not-found	25	13	4

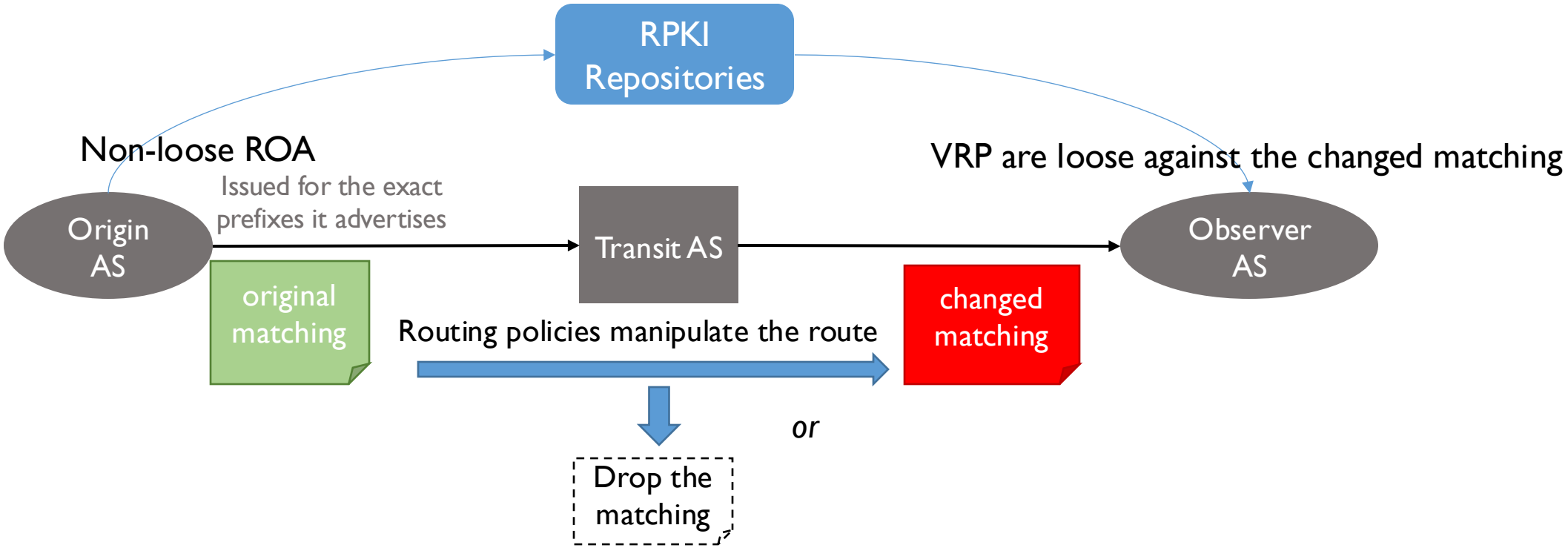
Observation 2: different types of partially visible matchings differ greatly in terms of ROV

Content

Q3: ***Why*** could partially visible matchings emerge?

Routing policies with hidden danger

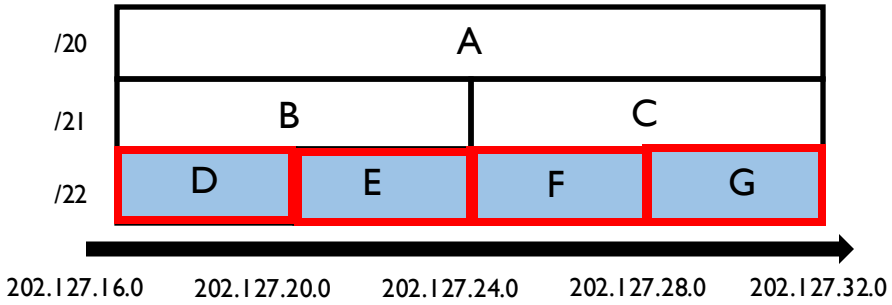
- Answer to Q3:
  - Certain BGP routing policies at *a transit AS* could manipulate a route's matching
  - The matching then becomes partially visible when it continues to spread from the transit AS to other observer ASes
  - We call such policies as "***policies with hidden danger***"



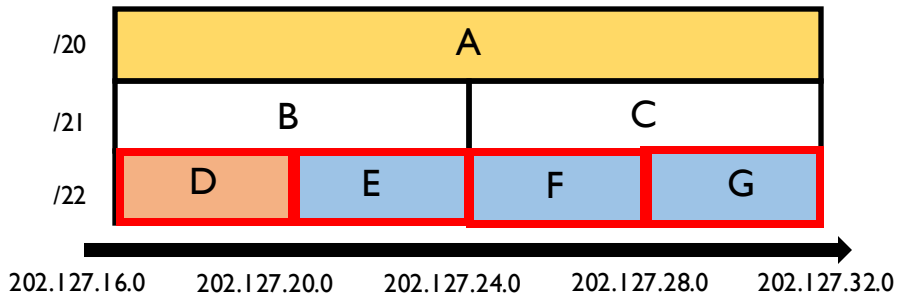
Types of routing policies with hidden danger

Type 1: explicit route filtering

- Typical policies:
  - Import / Export filtering
  - Route blackhole
  - Route damping
- Effect
  - Explicit Route filtering could contribute to ***unilaterally visible matchings***
  - Any address covered by the filtered prefix is vulnerable to super-prefix hijack and forged-origin hijack



Filter out D



- 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)

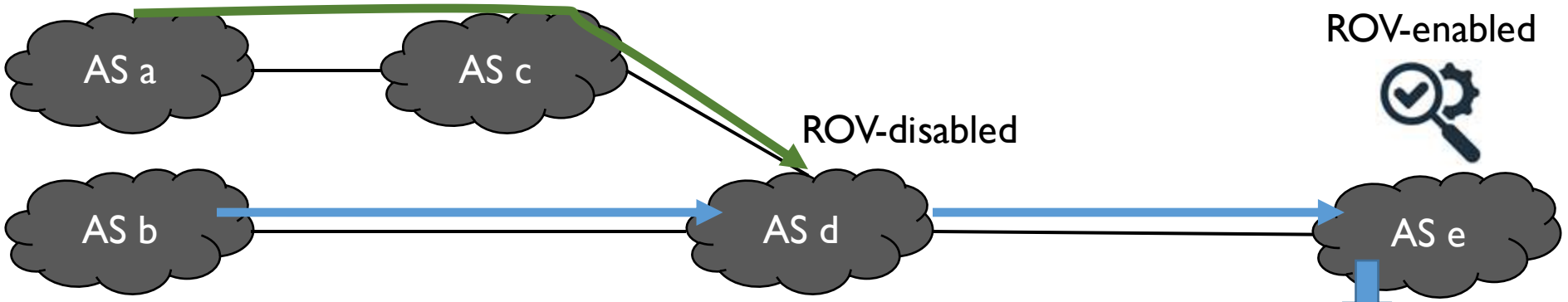
Prefix-origin matching of attack route in super-prefix hijack: AS 666, 202.127.16.0/20 (A)

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

Types of routing policies with hidden danger

Type 2: implicit route filtering

- A possible *combination* of routing policies:
  - (MOAS prefix with different origin ASes are announced, but only one matching issues ROA)
  - Route selection at the ROV-disabled router filters the valid route and keeps the invalid route
  - ROV-enabled router filters the invalid route
- Effect
  - There will be no route for any address covered by the prefix, so it is also vulnerable to super-prefix hijack and forged-origin hijack.



Both ASes advertise prefix p, but only AS a issues ROA

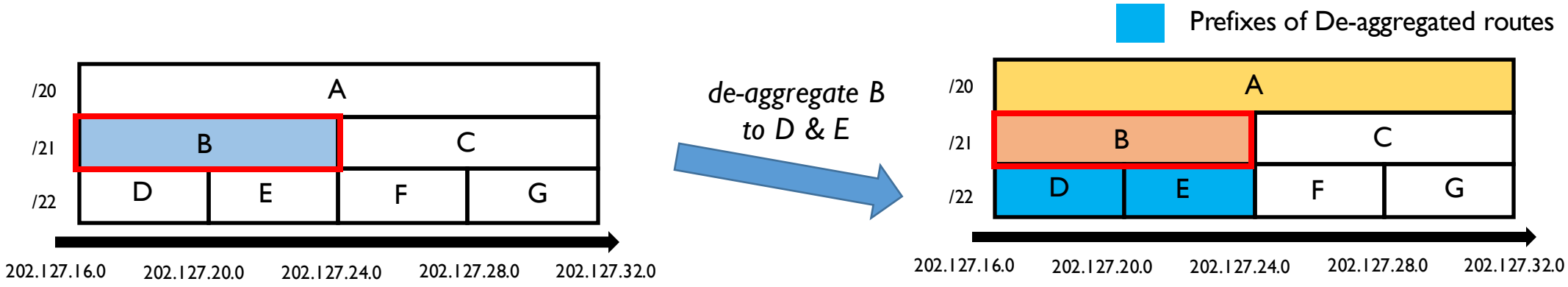
Route with prefix p from AS b is preferred, since b-d is shorter than a-c-d

The route is validated as invalid and gets dropped

Types of routing policies with hidden danger

Type 3: route de-aggregation

- 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
  - Route de-aggregation could generate ***DPSO*** matching pairs.
  - If de-aggregated prefix length is longer than its matching VRP's maxLength:
    - it will be validated as *invalid-length* and get dropped
    - the address covered by the de-aggregated prefix will also be vulnerable to super-prefix hijack and forged-origin hijack

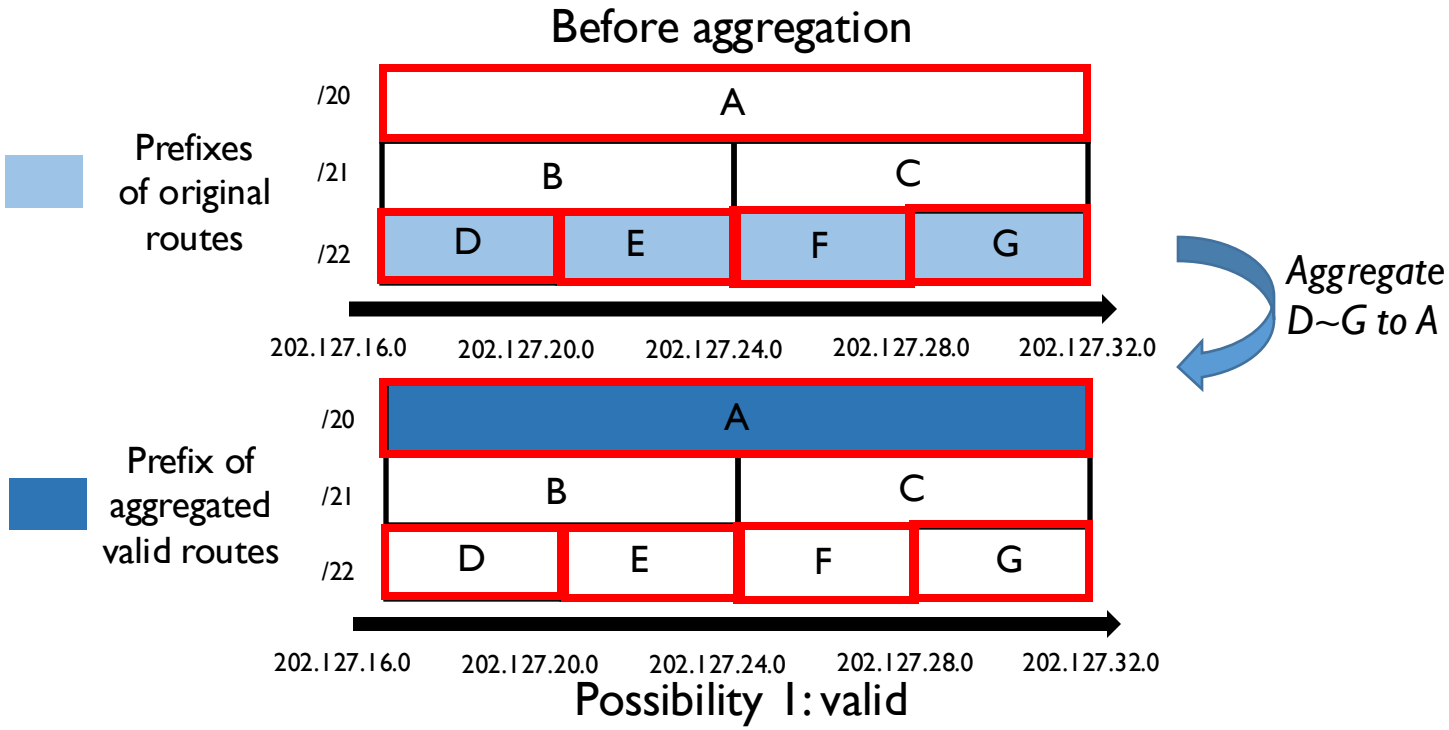


- VRP
  - VRP 1:AS 1, 202.127.16.0/21-21 (B)

Types of routing policies with hidden danger

Type 4: route aggregation

- Description
  - Route aggregation will *suppress* the original routes, and generate an aggregated route whose prefix is the super-prefix of all original prefixes
- Effect
  - Route aggregation could generate either DPSO or DPDO matching pairs.
  - The ROV state of the aggregated route could be one of all possible states.

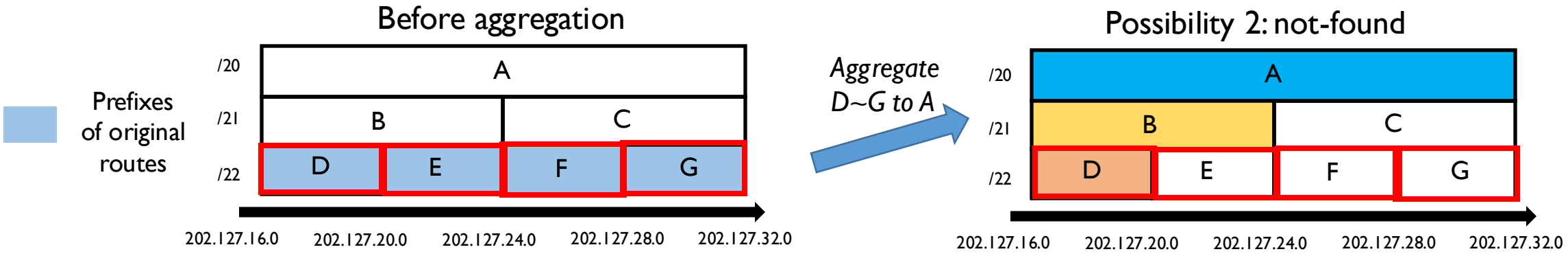


- VRP 1: AS 1, 202.127.16.0/22-22 (D)
- VRP 2: AS 2, 202.127.16.0/22-22 (E)
- VRP 3: AS 3, 202.127.24.0/22-22 (F)
- VRP 4: AS 4, 202.127.28.0/22-22 (G)
- VRP 5: AS 5, 202.127.16.0/20-20 (A)

Types of routing policies with hidden danger

Type 4: route aggregation

- Description
  - Route aggregation will *suppress* the original routes, and generate an aggregated route whose prefix is the super-prefix of all original prefixes
- Effect
  - Route aggregation could generate either DPSO or DPDO matching pairs.
  - The ROV state of the aggregated route could be one of all possible states.



- 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)
- No ROA issued for prefix A!

Prefix-origin matching of aggregated not-found route: AS5, 202.127.16.0/20(A)

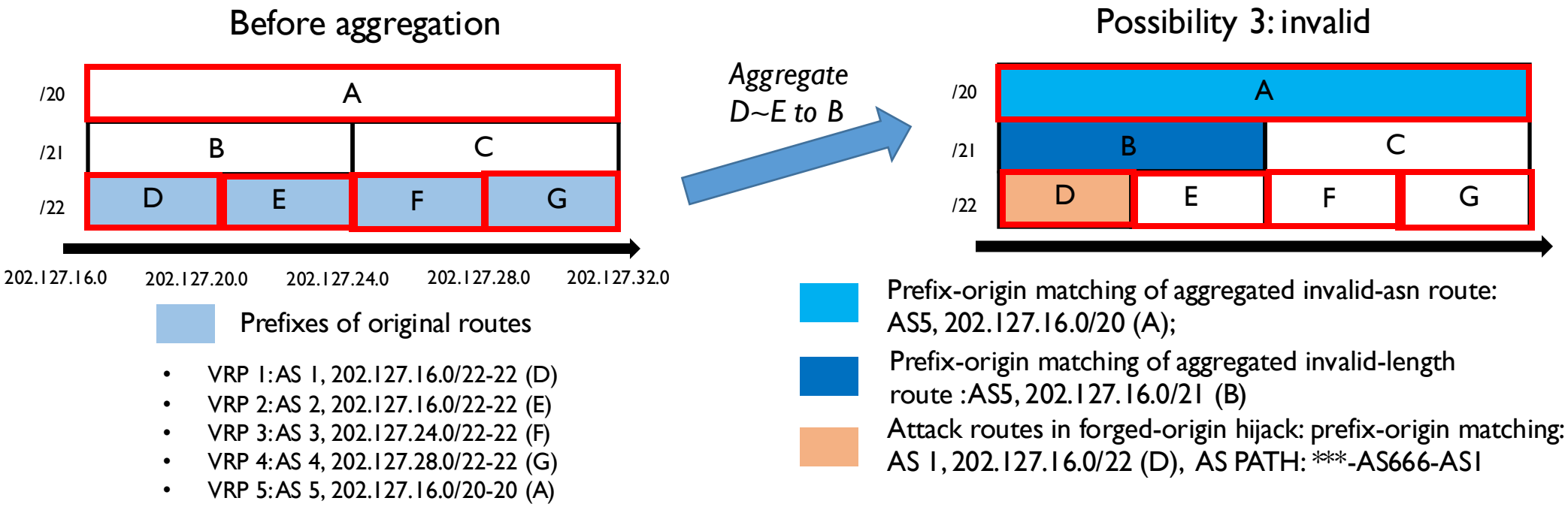
Prefix-origin matching of attack route in super-prefix hijack: AS 666, 202.127.16.0/21(B) → $20 \leq L < 22$

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

Types of routing policies with hidden danger

Type 4: route aggregation

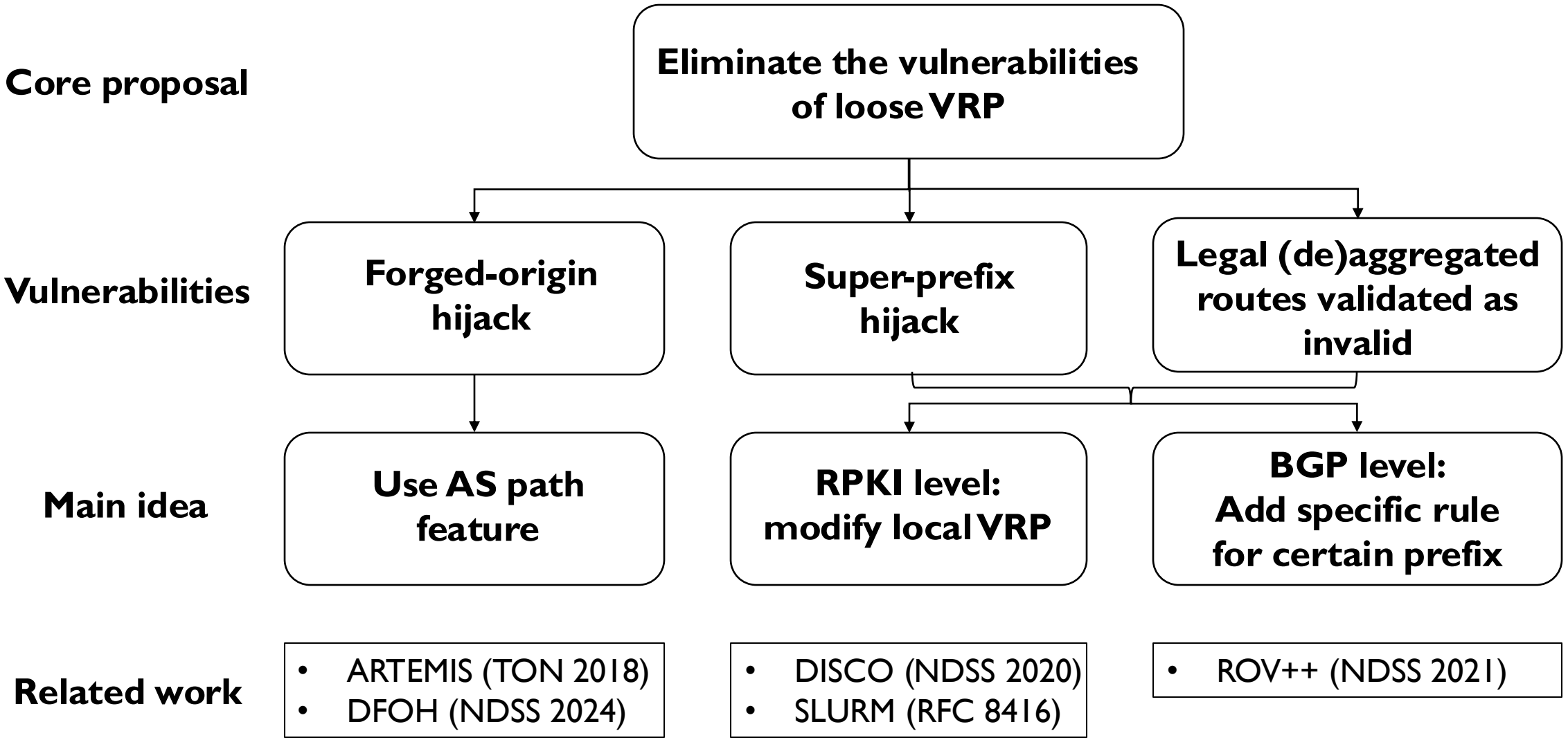
- Description
  - Route aggregation will *suppress* the original routes, and generate an aggregated route whose prefix is the super-prefix of all original prefixes
- Effect
  - Route aggregation could generate either DPSO or DPDO matching pairs.
  - The ROV state of the aggregated route could be one of all possible states.



Content

Q4: ***How*** to eliminate the inconsistency issue between the looseness of ROAs and VRPs?

Possible Solutions



Conclusions

- ✓ *Loose* ROA and VRPs are vulnerable to route hijacking including *super-prefix hijack* and *forged-origin hijack*.
- ✓ Non-loose ROAs *don't* necessarily lead to non-loose VRPs because observer ASes may fail to receive *partially visible matchings* of prefixes and their origin AS.
- ✓ There are multiple types of partially visible matchings, 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 eliminate the inconsistency issue between the looseness of ROAs and VRPs, the core proposal is to try to eliminate the vulnerabilities loose VRPs will bring.

Thank you!

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