Autonomous System Relationship Authorization (ASRA) as an Extension to ASPA for Enhanced AS Path Verification

Profile Draft: https://datatracker.ietf.org/doc/draft-geng-sidrops-asra-profile/
Verification Draft: https://datatracker.ietf.org/doc/draft-sriram-sidrops-asra-verification/

K. Sriram

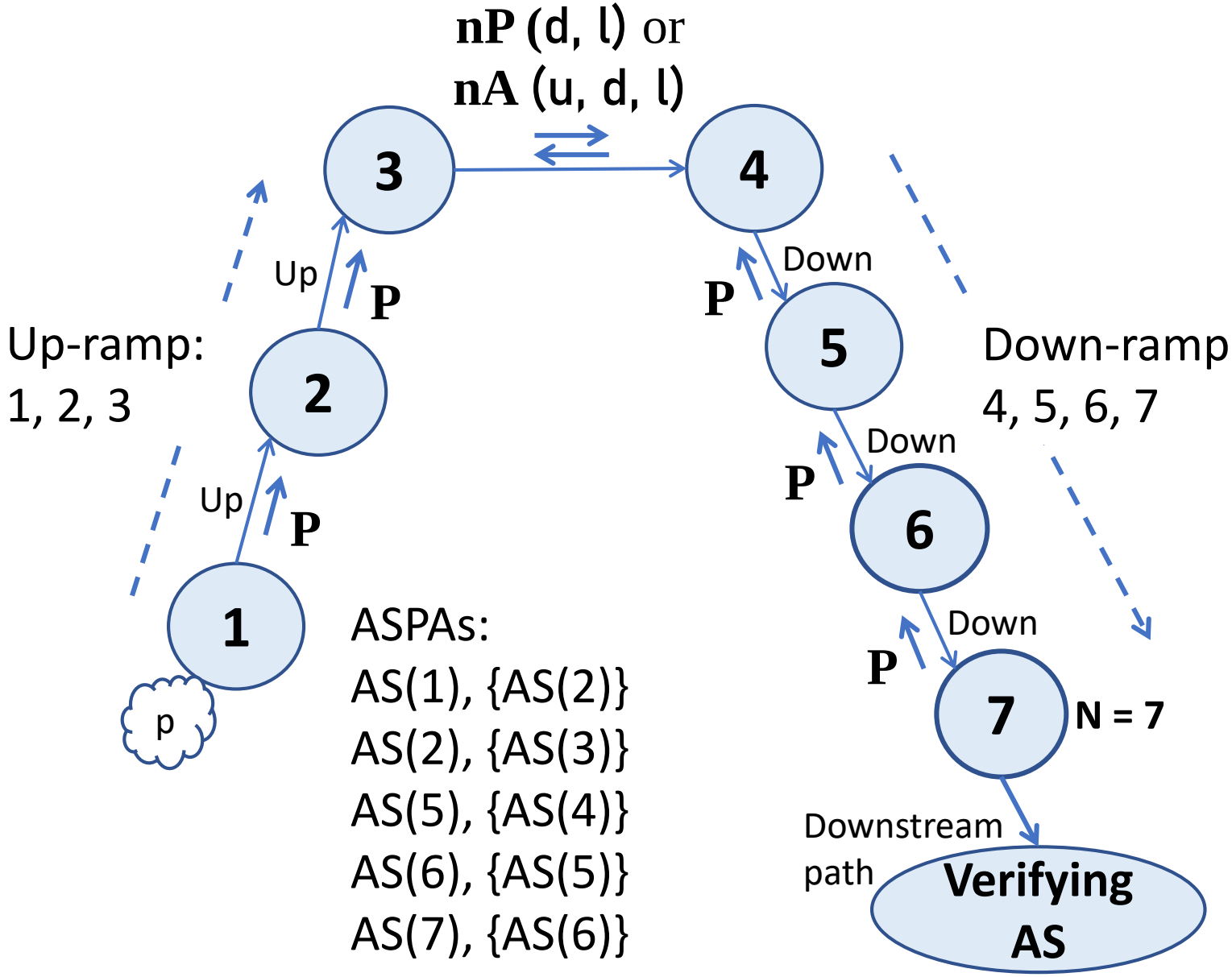
Authors: Kotikalapudi Sriram, Nan Geng, Amir Herzberg, Mingqing Huang

SIDROPS Meeting, IETF 121
November 2024

Problem Statement

- ASPA-based AS path verification can detect all route leaks
- It can also detect **forged-origin and forged-path-segment hijacks** when Update is received from a customer or lateral peer
  - **These are essentially fake-link (or forged-peering) attacks**
- Goal:
  - Detect and mitigate fake-link attacks received from any direction (i.e., Update received from a provider or customer or lateral peer)
  - ASPA's route leak detection capability **must** remain intact

ASPA Verification of Downstream AS Path: Valid Outcome



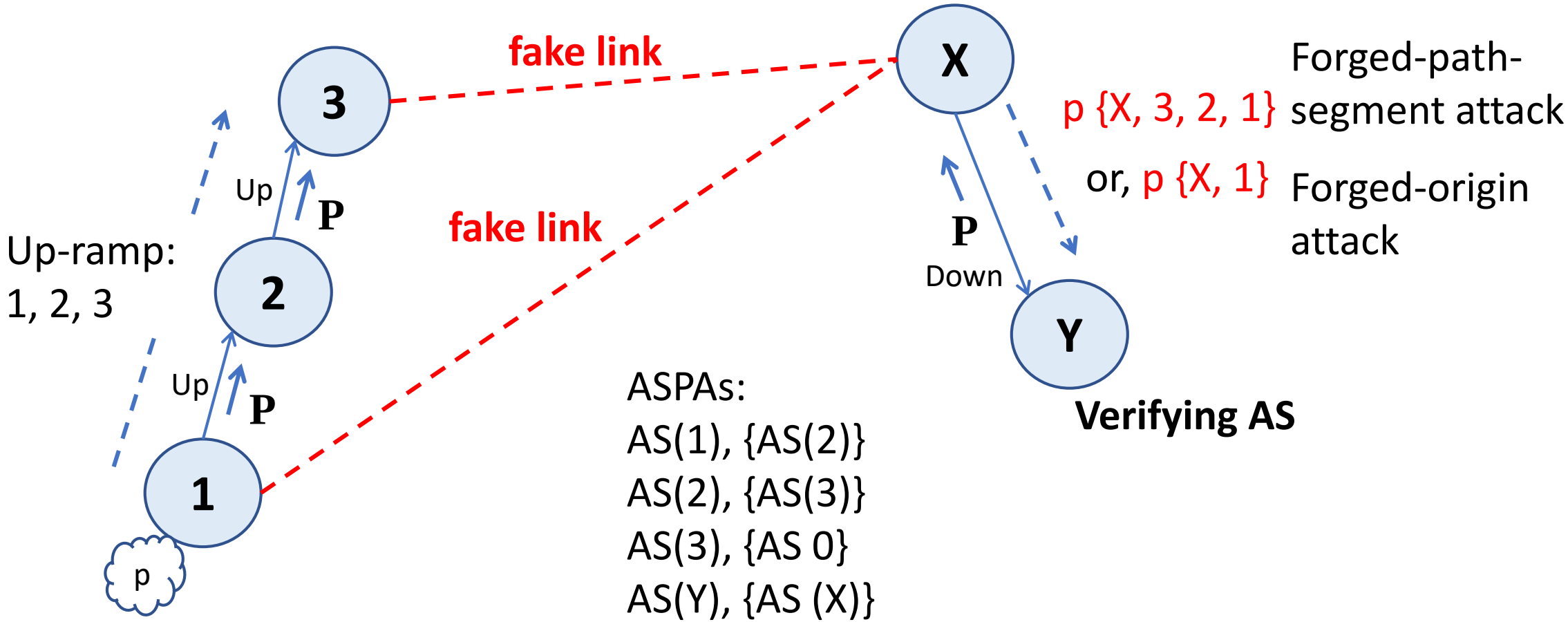
Shortcoming:
The verifying AS cannot tell if AS 4 is faking a link to AS 3

P: Provider
nP: not Provider
nA: no Attestation

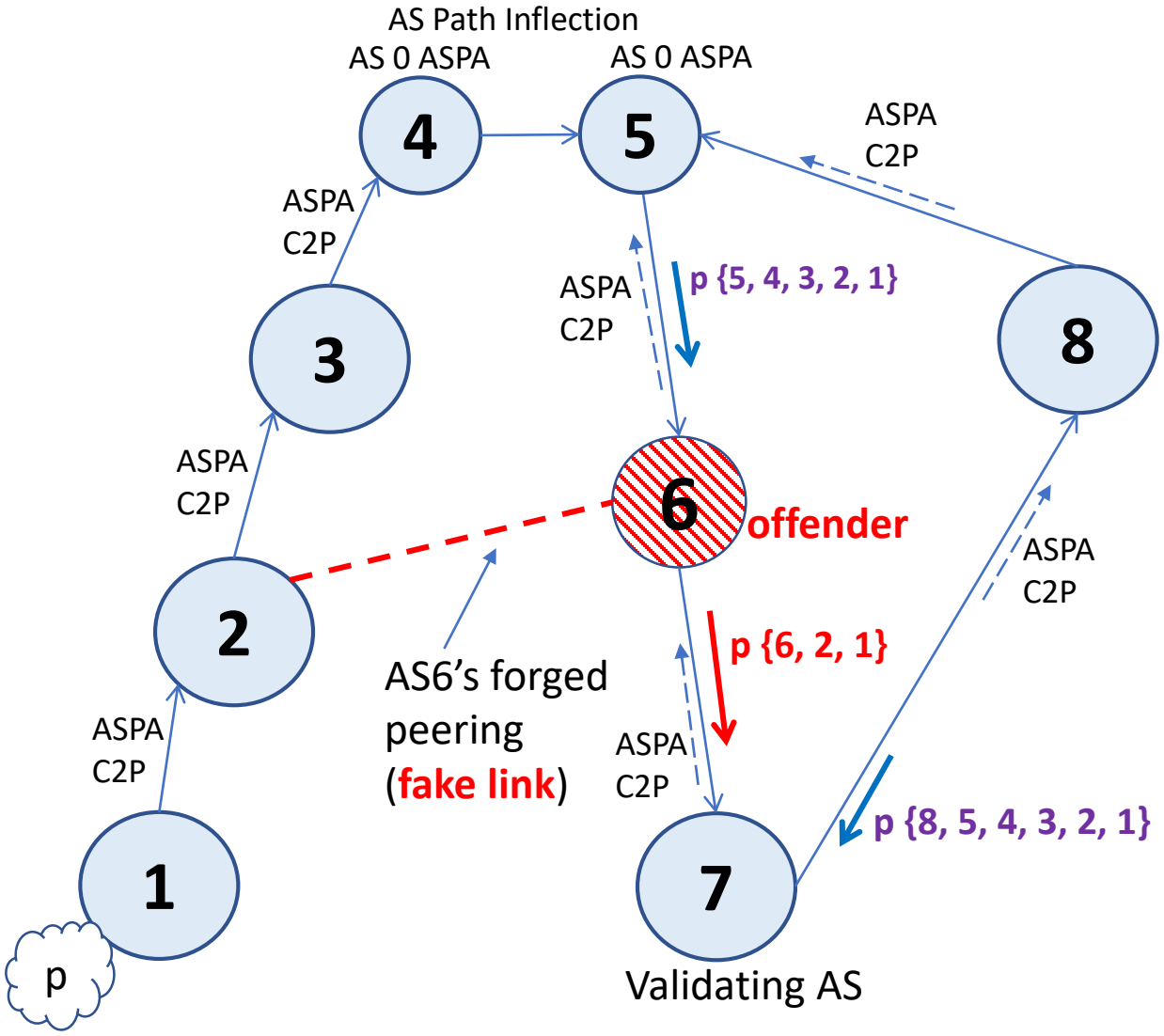
u = Up (customer to provider (C2P))
d = Down (provider to customer (P2C))
l = Lateral (peer to peer (p2p))

Fake-Link Attack

- ASPA verification not checking the AS hop at the top leaves room open for fake-link attacks



AS_PATH maliciously shortened by a Provider

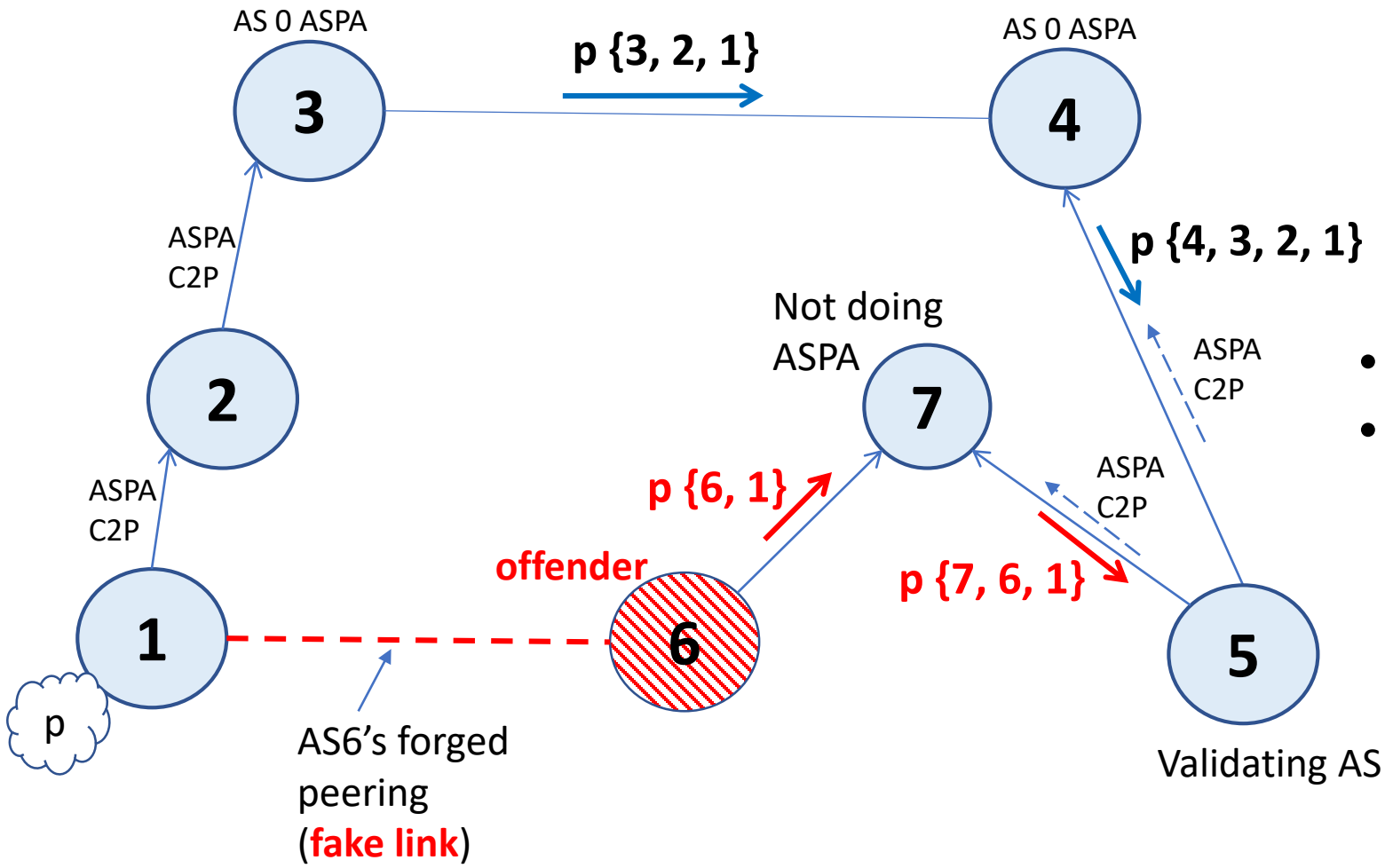


C2P = Customer to Provider

- All ASes are doing ASPA
- AS6 (provider) wants AS7 (customer) to prefer its path
- AS6 shortens the AS_PATH
- AS6 does not intend to drop data traffic from AS7 (if it does, that can be addressed only at a higher layer)
- Consider path validation at AS 7

ASPA deficiency: AS6 can shorten the path as shown w/o detection. ASPA verification cannot verify the physical existence of the AS3 to AS6 (or AS2 to AS6) hop* (the presumed inflection hop).

Customer Attacking its Provider and Provider's other Customers in turn



- Partial deployment
- AS 7 not doing ASPA

C2P = Customer to Provider

Solution

- New RPKI object: Autonomous System Relationship Authorization (ASRA)
- Allows for registration of customers and lateral peers
- Either ASPA or ASRA must confirm a BGP peering (BGP link) with the next AS at each hop in the AS path in forward direction
  - E.g., consider AS(i) to AS(i+1) to be a fake-link if AS(i)'s ASPA and ASRA both exist and neither attests to a relationship with AS(i+1)
- ASPA-alone method's guarantee is that the AS path is feasible
  - ASPA+ASRA method's additional guarantee is that fake-link (or forged-peering) attacks are detected

ASRA Subcategories

- Three subcategories of ASRA: ASRA1, ASRA2, ASRA3
- ASRA1 is used by the subject AS to register all customers
- ASRA2 is used by the subject AS to register all lateral peers
- ASRA3 is an alternative to ASRA1 and ASRA2 in case the subject AS is not willing to disclose its customers explicitly
- ASRA3 is used by the subject AS to register a combined list of all customers and lateral peers without differentiation

ASRA Subcategory Formalized in the ASN.1

```
ct-ASRA CONTENT-TYPE ::=
  { TYPE ASRelationshipAttestation IDENTIFIED BY id-ct-ASRA }

ASRelationshipAttestation ::= SEQUENCE {
  version [0]   INTEGER DEFAULT 0,
  SignerASID  ASID,
  ASRAsubcategory  subcategory,
  Relationships     RelationshipASSet

ASID ::= INTEGER (0..4294967295)
subcategory ::= OCTET STRING (SIZE (1))
RelationshipASSet ::= SEQUENCE (SIZE(1..MAX)) OF ASID
```

ASRA Registration Recommendations

- A subject AS that has ASRA MUST also have ASPA
  - ➢ They are only useful together to confirm a fake link
- ASRA without ASPA for a subject AS MUST be ignored in AS path verification
- An ASRA-compliant AS MUST either register ASRA3 alone or register both ASRA1 and ASRA2
- If ASRA3 exists along with ASRA1 and ASRA2 for a subject AS, then only the ASRA3 MUST be considered for AS path verification and ASRA1 and ASRA2 MUST be ignored

ASRA Registration Recommendations

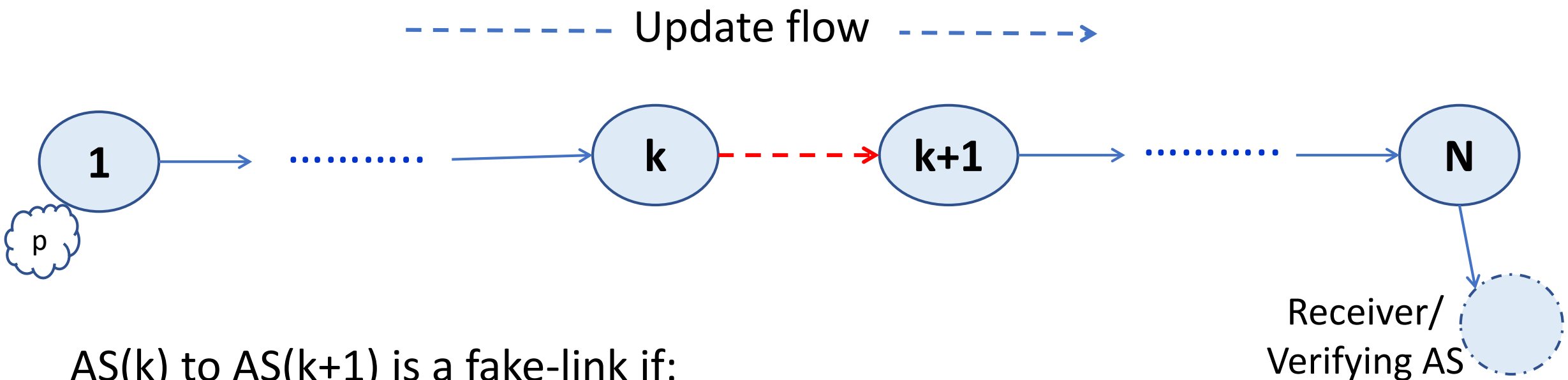
- To signal that there are no neighbors to report in a subcategory, only AS 0 **MUST** be included in an ASRA of the corresponding subcategory in the RelationshipASSet field
- Details of requirements for registration of ASRA for mutual transit ASes, complex relationship ASes, and route server ASes are also specified in the draft (Sec. 3)

AS Path verification based on ASPA & ASRA

Algorithm Principles

- Preserve how ASPA by itself detects **Invalid** outcome
- Only when ASPA has determined an AS_PATH to be **Valid** or **Unknown**, apply additional verification using ASRA
- ASPA and ASRA are together used to determine if the AS_PATH has a fake link
- For any hop in the AS_PATH, ASRA in the direction opposite to Update flow is never invoked in path verification
  - ➢ This preserves the sanctity of ASPA (i.e., DO NOT meddle with ASPA's route leak detection capability)

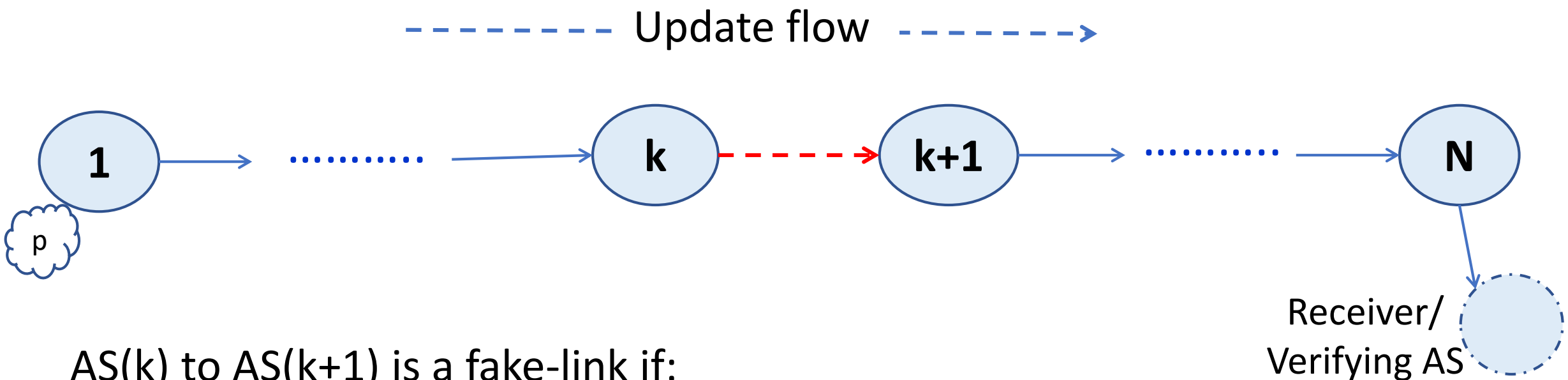
Fake-Link Detection: Algorithm A



AS(k) to AS(k+1) is a fake-link if:

- {ASPA of AS(k) exists and does not include AS(k+1)} AND
- {ASRA of AS(k) exists and does not include AS(k+1) as a customer or lateral peer} AND
- {Either ASPA of AS(k+1) does not exist OR it does not include AS(k)}

Fake-Link Detection: Algorithm B



AS(k) to AS(k+1) is a fake-link if:

- {ASPA of AS(k) exists and does not include AS(k+1)} AND
- {ASRA of AS(k) exists and does not include AS(k+1) as a customer or lateral peer}

Combined ASPA+ASRA Verification of Downstream AS Path

1. Perform AS path verification based on ASPA alone
   - Outcome: Invalid, Valid, or Unknown
2. If the outcome is Invalid, it remains unchanged and the procedure halts
3. Else, if a fake link was detected (by applying Algorithm A or B):
   - Valid or Unknown (per ASPA at Step 1) → Invalid and the procedure halts
4. Else, Valid or Unknown (per ASPA at Step 1) remains unchanged and the procedure halts

Benefits to Early Adopters

- Incremental benefit is accrued by early adopters
- An AS that deploys ASPA and ASRA prevents an offending AS from faking a link to it if the receiving/verifying AS also deploys ASPA and ASRA
  - Independent of whether or not intermediate ASes adopt ASPA or ASRA

Operational and Security Considerations

- A number of recommendations are stated in the Operational Considerations section concerning keeping ASPAs and ASRAs current, correct, and complete
- These are important for functionality as well as security

Thank you.

Questions / Comments?