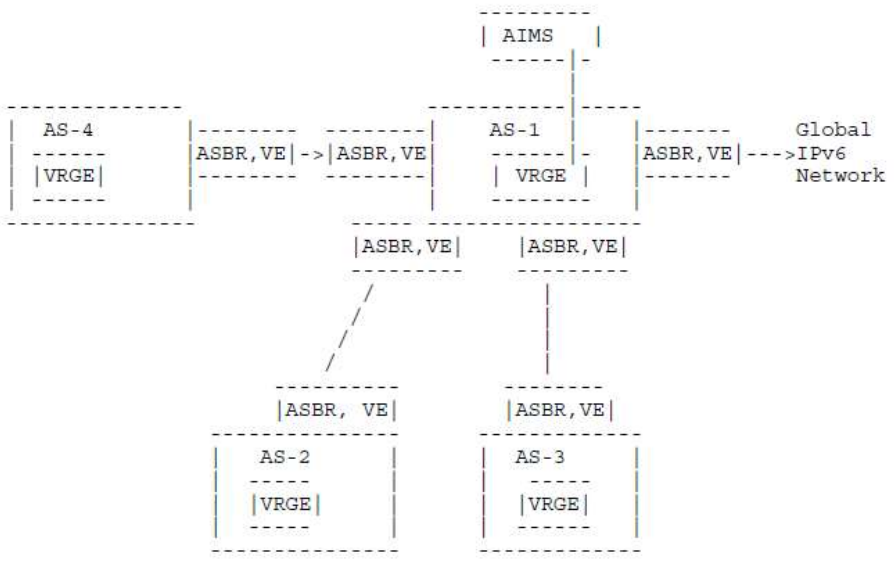
Inter-domain Source Address Validation based on AS relationships

Gang Ren, Shuqi Liu, Xia Yin
Tsinghua University

Background

- **Inter-domain Source Address Validation** plays a significant role in relieving the source IP address spoofing. Several solutions have been proposed.
- **AS relationships mainly determine routing exporting rule between AS**, so AS relationships can be used to generate approximate source address validation rules.
- We have proposed the original idea of validation scheme based on AS relationships in **RFC5210**.
- People have higher tolerance for false filtering but lower acceptance for false blocking.
- We hope to propose a **lightweight** scheme with moderate accuracy, convergence speed and cost compared to existing algorithms.



RFC 5210-Figure 3: Inter-ISP (Neighboring AS) Solution

Major AS Relationships

- **Provider to Customer relationship** (P2C relationship, Transit relationship)
- **Peer to Peer relationship** (P2P relationship)
- **Sibling to Sibling relationship** (S2S relationship)

	Peer	Provider	Customer	Sibling	Self
To Peer			√	√	√
To Provider			√	√	√
To Customer	√	√	√	√	√
To Sibling	√	√	√	√	√

Fig 1. Exporting rule table of major AS relationships.

- An AS exports the address prefixes of itself, its customers, its providers, its siblings, and its peers to its customers and siblings as valid prefixes, while it only exports the address prefixes of itself, its customers, and its siblings to its providers and peers as valid prefixes.

Incidental Complex AS Relationships (1)

- **Hybrid relationship**: Two ASes have different relationships at different interconnection points (e.g. P2C in one location and P2P elsewhere).

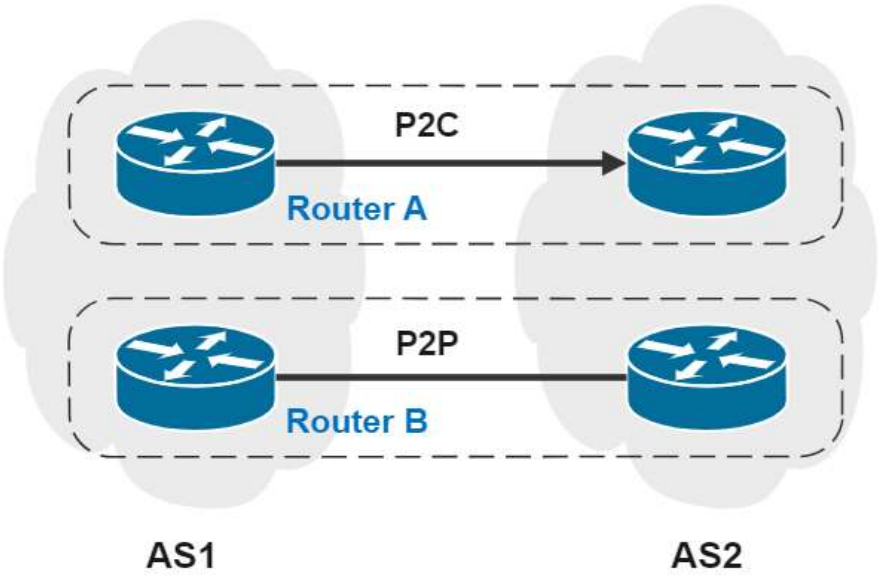


Fig 2. An example of Hybrid relationship.

Incidental Complex AS Relationships (2)

- **Partial Transit relationship** : An AS offers another AS transit to its peers and customers, but not providers.

	Peer	Provider	Customer	Sibling
To Partial-Customer	√		√	√

	Peer	Provider	Customer	Sibling
To Partial-Provider			√	√

Fig 3. Exporting rule table of partial transit relationship.

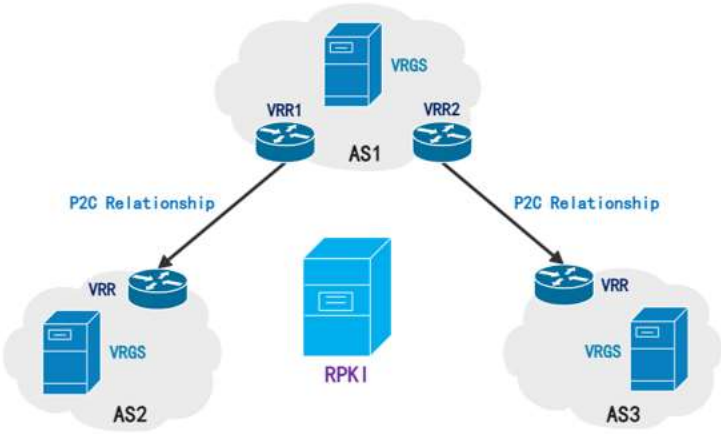
- Other incidental complex AS relationships…

AS Relationship Acquisition Methods

- **Inference Algorithms**: These algorithms use various data to infer AS relationships. According to different strategies they use, they can be mainly divided into three types, namely Network feature ranking algorithms, Combinatorial optimization algorithms and Partial determination algorithms.
- **Querying approach**: The set of ASes which are in P2C/C2P relationship with one AS can be straightly obtained from ASPA objects in RPKI. Newly proposed ASRA idea can record more complex information of various AS relationships, and may help with our scheme.
- **Internal Announcement**: ASes running related validation mechanisms directly declare their relationships to each other.

Static Architecture

- **Validation Rules Generation Server (VRGS)**
  - VRGS exchanges validation rules with VRGS of other ASes.
  - VRGS obtains IP address prefixes corresponding to ASN from RPKI.
  - VRGS sends the prefix validation rule table to Validation Router.
- **Validation Router (VRR)**
  - VRR deploys validation rules to verify source addresses of packets.
  - VRR receives new rules from VRGS to update its validation rule table.
- **The Mapping from ASN to IP address prefixes owned by the AS**
  - The mapping from ASN to IP address prefixes owned by the AS can be support by Resource Public Key Infrastructure (RPKI) .



Relative Data Structure

- **Neighbor AS Table**
  - This table stores ASN, AS relationship and ASN validation rule set of every neighbor AS.
  - Recorded in VRGS.

AS Number	AS Relationship	Permissible AS Number
ASN1	P2C	ASN1,ASN3
ASN2	P2P	ASN2,ASN4

Fig 4. An example of neighbor AS table.

- **Prefix Validation Rule Table**
  - This table stores the set of valid source address prefixes.
  - Recorded in both VRR and VRGS.

Permissible Prefixes	Prefixes Set1

Fig 5. An example of prefix validation rule table.

- **Static Exporting Rule Table**
  - This table stores exporting rules of AS relationships.
  - Recorded in VRGS. See Fig 1.

Update Circumstance (1)

- **Change of the AS relationship**
  - When changes occur to the relationships between two ASes, VRGSes of two ASes both need to update the ASN validation rule set in their **Neighbor AS Table**.

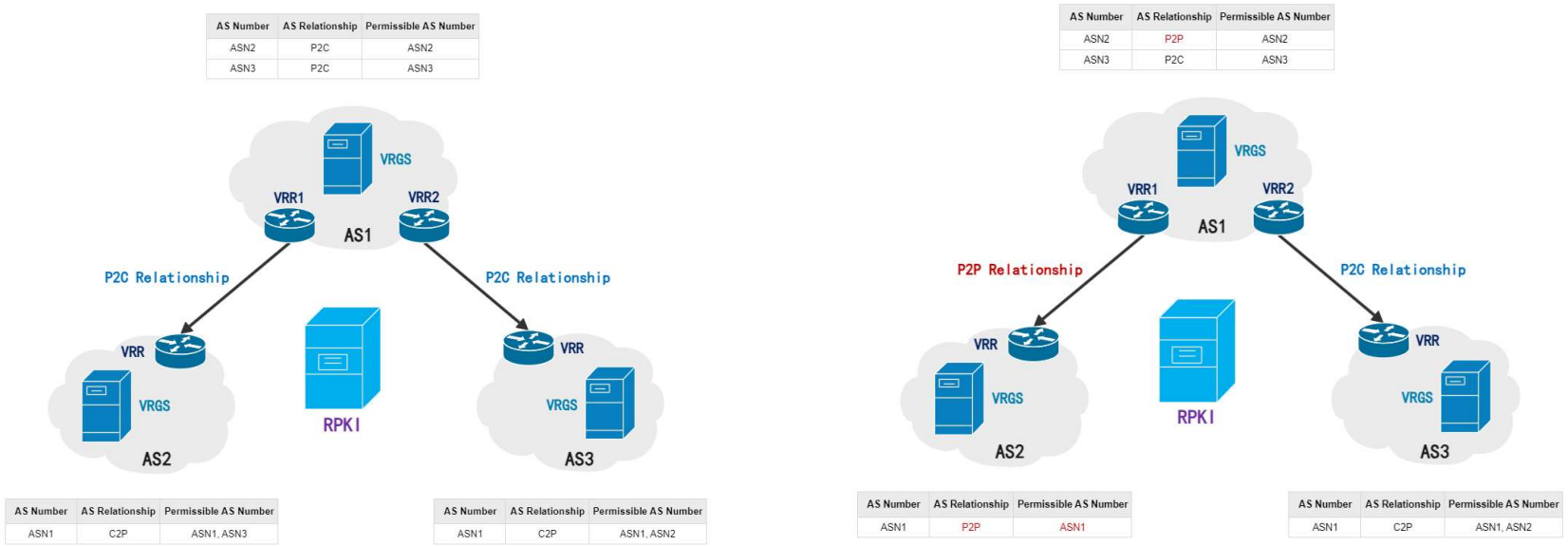


Fig 6. An example of AS relationship change.

Update Circumstance (2)

- **Change of the prefixes of AS**
  - VRGS needs to regenerate its **Prefix Validation Rule table** based on the new mapping, and deploy the new prefix validation rule table on its corresponding VRR.

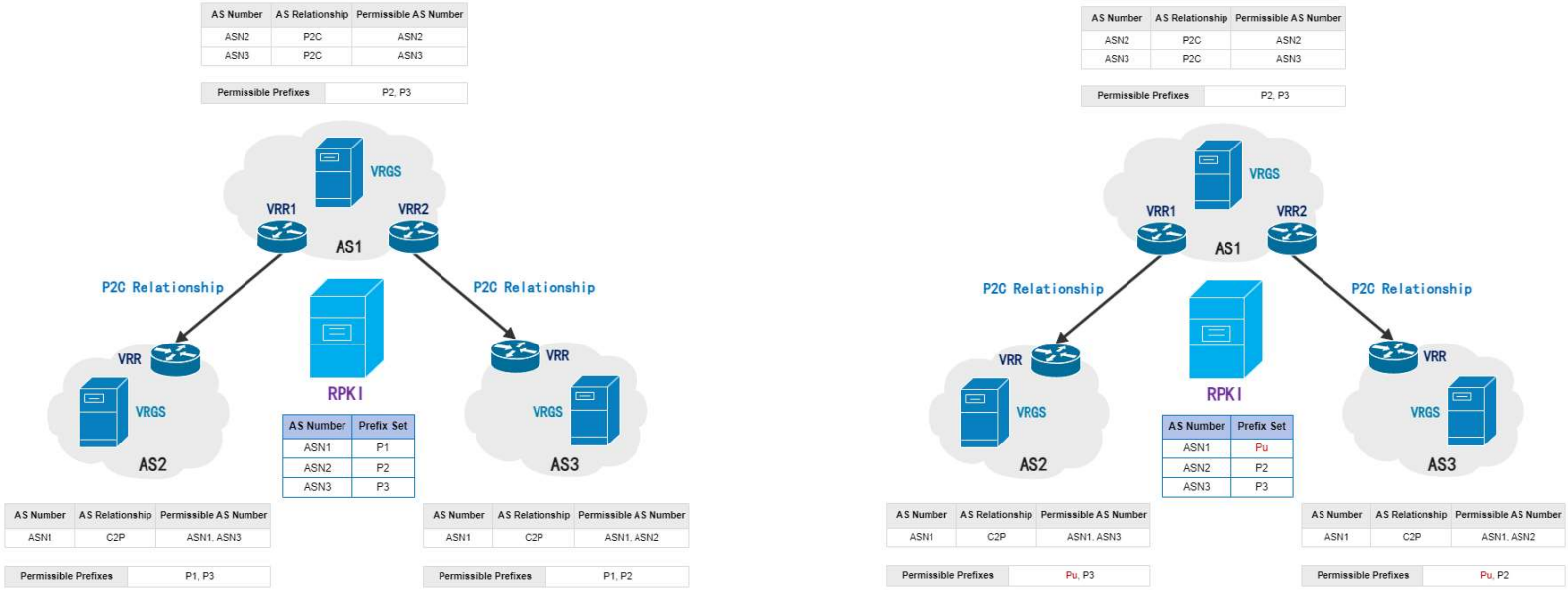


Fig 7. An example of AS prefixes change.

Update Circumstance (3)

- **Change of the network topology**
  - **Only if** AS relationships change with the network topology, validation rules recorded in relative ASes will change.
- **Change of the routing information**
  - **Only if** AS relationships change with the routing information, validation rules recorded in relative ASes will change.

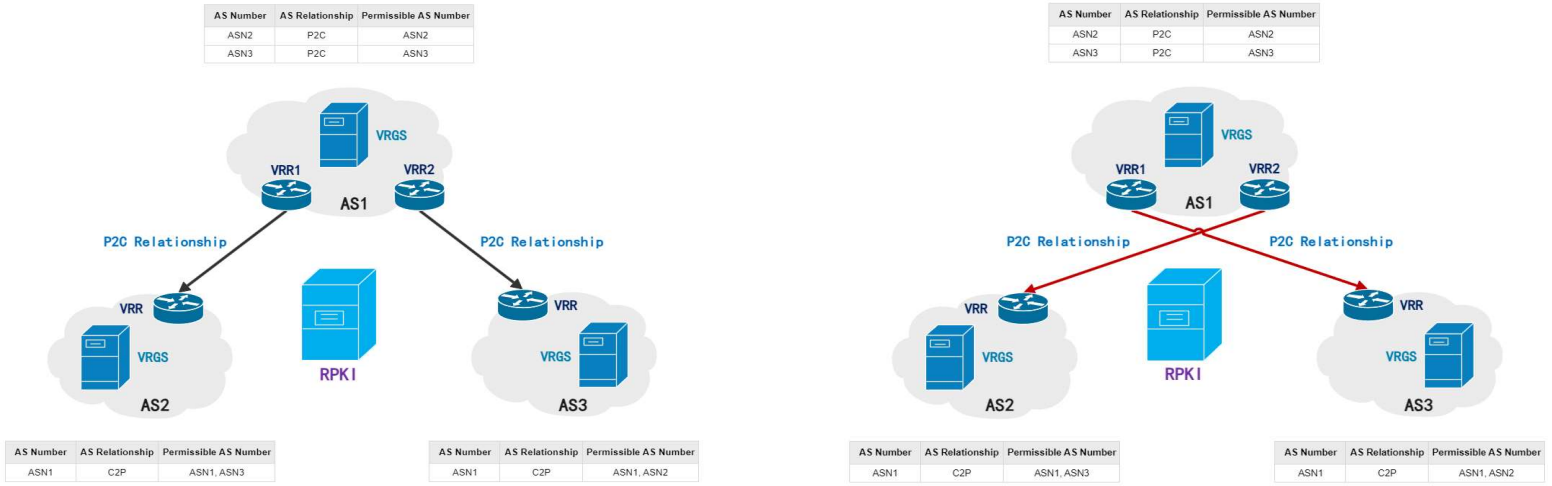


Fig 8. An example of network topology change.

Design Considerations on Deployability

- **Relatively stable**
  - The updates are mainly triggered by change of the AS relationships and change of the prefixes of AS.
- **Utilize existing information as much as possible**
  - Using the existing information from AS relationship and RPKI.
- **Prefer to use and exchange more abstract information**
  - AS numbers rather than fine-grained IP prefixes are transmitted by the solution.
- **Try to balance accuracy, time and cost**
  - An easily deployable lightweight validation scheme requires a balance between accuracy, cost and convergence time.

Next Step

- A new protocol or extension based on BGP4 and the security considerations.
- Special processing mechanisms for various incidental complex AS relationships and corner cases.
- Solution on inaccurate mapping from AS to IP address prefix and inaccurate information from RPKI.
- Evaluation models and metrics that balance deployment overhead and accuracy.

Thank you for listening