Inter-domain Source Address Validation based on AS relationships

draft-rly-savnet-inter-domain-as-relationships-03

Gang Ren, **Shuqi Liu**, Xia Yin

Tsinghua University

SAVNET Meeting, IETF 122

March 2025

Brief History

- **Main Motivation**
  - Use AS relationships as the abstraction of inter-domain routes
  - Avoid improper block, and balance accuracy and cost
- **Previous Work**
  - RFC 5210, divided SAV into three levels: the access network, intra-domain, and inter-domain, and proposed original idea of AS relationships based SAV in inter-domain level
  - draft-rly-savnet-inter-domain-as-relationships-00, June, 2023
  - draft-rly-savnet-inter-domain-as-relationships-01, IETF 118 SAVNET WG
  - draft-rly-savnet-inter-domain-as-relationships-02, December, 2024
  - draft-rly-savnet-inter-domain-as-relationships-03, IETF 122 SAVNET WG

Comments from chair and Updates

- **Comment 1.** Draft-01 uses a new centralized server, suggest considering modifications
  - **Response:** We update the design in Section 3. We change to a distributed SAV scheme and implement it on existing routers.
- **Comment 2.** Draft-01 uses a new protocol to communicate between centralized servers, suggest considering modifications
  - **Response:** We add a feasible implementation in Section 4. We extend existing BGP protocol to advertise SAV rules.

Comments from chair and Updates

- **Comment 3.** Consider merging with another scheme [draft-song-savnet-inter-domain-bgp-ops]
  - **Response:** After comparison and discussion, we keep them separate as they differ in requirements, architecture, and use cases.
- **Other Main Updates**
  - We add the analysis of the SAV system in some multi-homing scenarios in Section 5, including multipoint interconnection and limited propagation scenarios.

AS relationships

- **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	√	√	√	√	√

AS relationships

- **Incidental AS Relationships**
  - Hybrid Relationship: different relationships at different interconnection points
  - Partial Transit Relationship: restricts the scope of a typical P2C relationship to the provider AS's peer ASes and customer ASes (but not provider ASes)

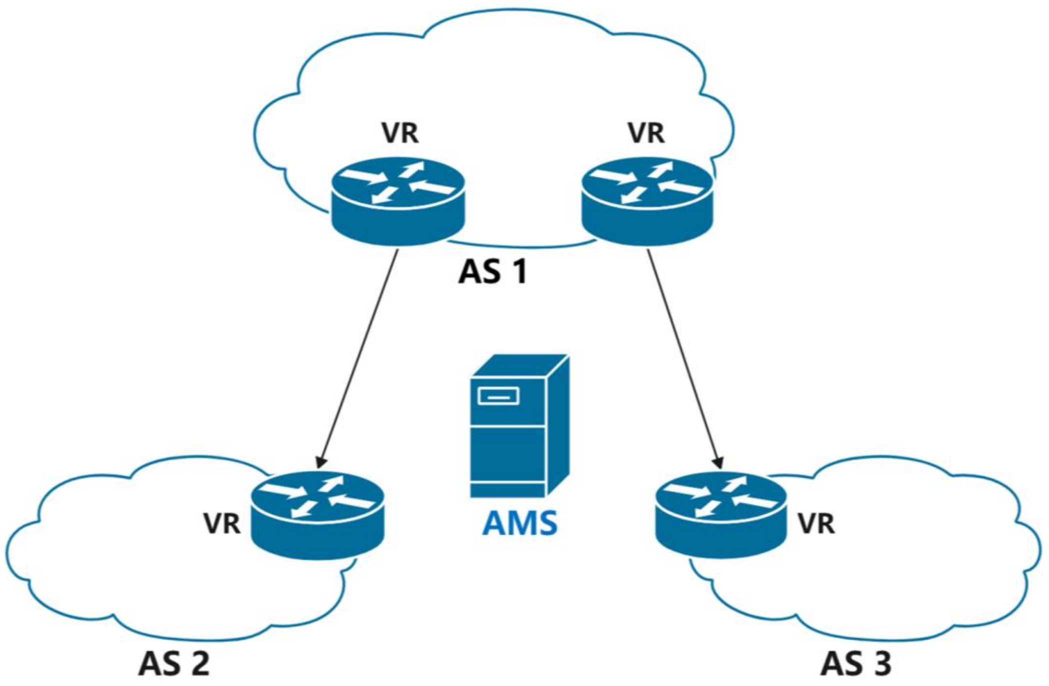
- **AS relationship acquisition methods**
  - Direct announcement between neighbor ASes deploying SAV.
  - Inference algorithms such as AS Rank[1], Problink[2].
  - Query methods like using ASPA objects.

[1] Luckie M, Huffaker B, Dhamdhere A, et al. AS relationships, customer cones, and validation[C]//Proceedings of the 2013 conference on Internet measurement conference. 2013: 243-256

[2] Jin Y, Scott C, Dhamdhere A, et al. Stable and practical {AS} relationship inference with {ProbLink}[C]//16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19). 2019: 581-598.

Architecture

- **Validation Router (VR)**
  - Existing border routers act as VRs, and are responsible for ASN and IP prefix SAV rule generation (VRGE in draft-01 is removed) and packet validation.
  - VRs generate IP Prefix SAV Rules based on ASN SAV Rules by querying AMS
- **Address Mapping Server (AMS)**
  - AMS records the mapping from ASNs to IP address prefixes owned by ASes
  - The information can be calculated using ROA objects from the RPKI

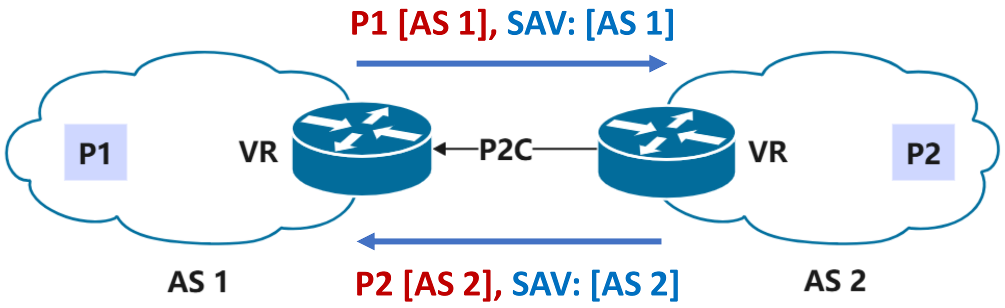


BGP Extension

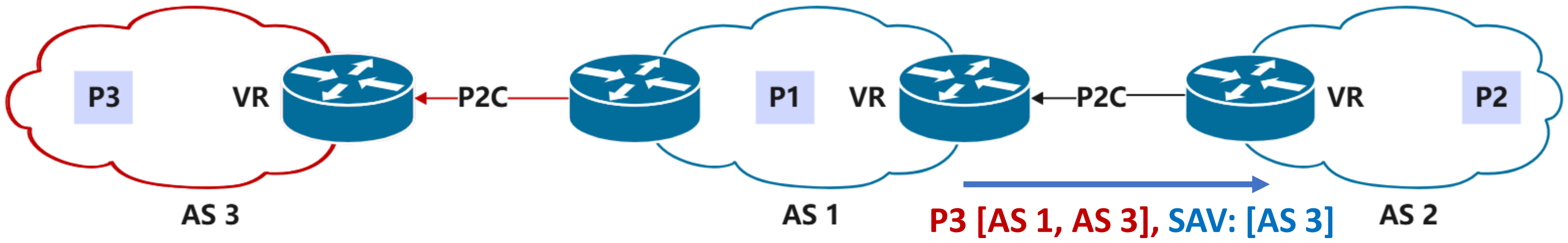
- VRs can advertise SAV rule updates with BGP UPDATE messages
- A newly designed BGP path attribute to transfer ASN SAV rules
  - <type, length, value>, and the value field carries ASN sets

1. Initial BGP UPDATE messages carry initial routes and SAV rules.

2. AS 1 accepts new routes and SAV rules from AS 3.



3. AS 1 sends a BGP UPDATE message carrying updated routes and SAV rules to AS 2.



Dynamic Scenarios

- **Scenario 1:** AS Relationships Change
  - ASN SAV rules update. IP Prefix SAV rules update accordingly.
- **Scenario 2:** AS Prefixes Change
  - ASN SAV rules remain unchanged. IP Prefix SAV rules update accordingly.
- **Scenario 3:** AS Network Topologies Change
  - ASN SAV rules update. IP Prefix SAV rules update accordingly.
- **Scenario 4:** BGP Attributes Change
  - ASN SAV rules remain unchanged. IP Prefix SAV rules remain unchanged.
- The system handles AS level updates and ignores fine-grained updates.

Considerations on Deployment

- Utilize existing information as much as possible
  - ➢ Using new information brings more costs and higher deployment demands.
- Prefer to use and exchange more abstract information
  - ➢ Using abstract information reduces costs and improves efficiency, which is more conducive to promoting the SAV scheme deployment.
- Balance accuracy, time and cost
  - ➢ To be better deployed in practice, schemes should balance accuracy, cost, and convergence time well.

New comments from chair

- **7 new comments** are proposed recently
  - **3 comments** focus on the **comparison** between our scheme and **BAR-SAV**.

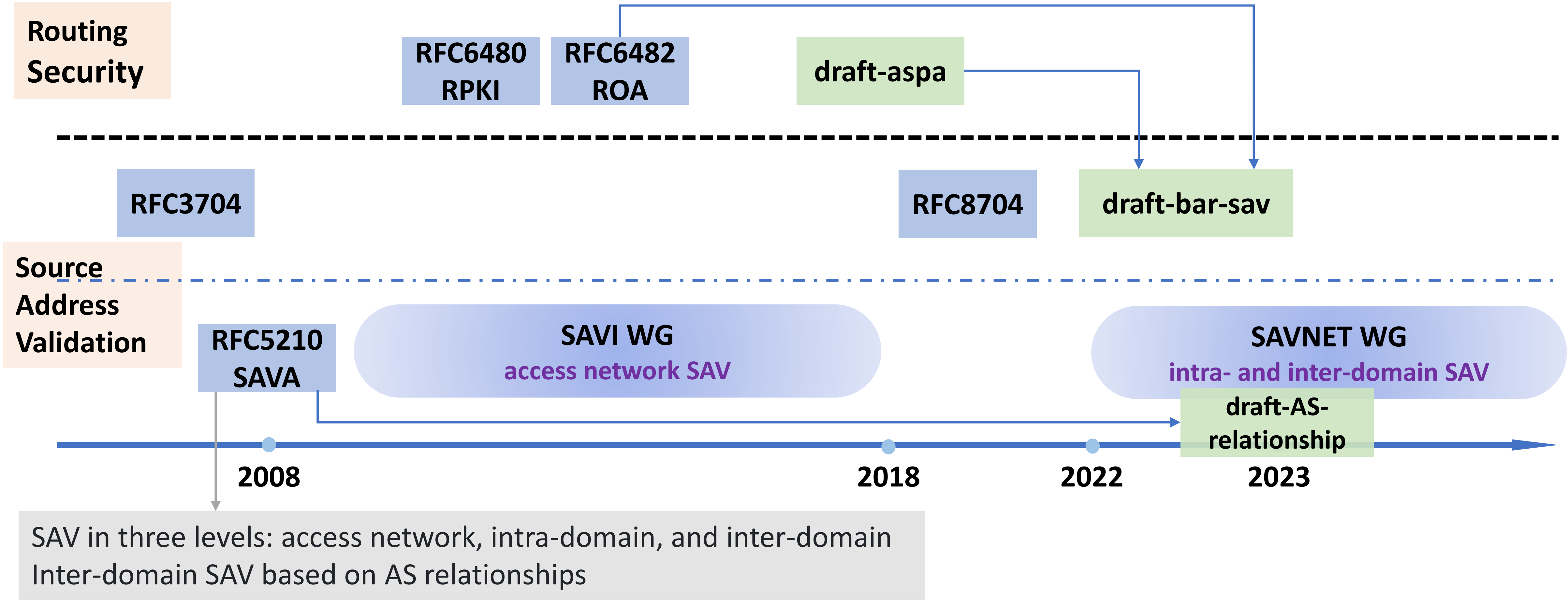
    1) If the information of AS relationship is coming from also ASPA, then what's the main Pros/Cons of your solutions when compared with BAR-SAV

    2) If such information is not from ASPA, then how can you assure the coverage and accuracy of such information?

    4) It seems that "AMS" has the same aim of ROA on RPKI? If so, would you like to use the ROA directly?
  - **4 comments** are about the writing of our draft. We will clarify the definition of different terms and modify those unclear descriptions in future updates.

Develop Timeline

- Based on the same principle, we achieve the same goal through different paths.



Comparison with BAR-SAV[1]

	Scheme based on AS relationships	BAR-SAV
How to obtain AS relationships	Use AS relationships announced between neighbor ASes. Take other methods as feasible alternatives.	ASPA and/or BGP UPDATE
How to establish possible source AS sets	Propagate updates with BGP extension. After receiving updates, calculate further propagation with export rules.	Query ASPA at a single point
How to convert AS sets into prefix lists	Convert by querying AMS. Currently, ROA in RPKI is a feasible implementation of AMS.	ROA and/or BGP UPDATE

[1] draft-ietf-sidrops-bar-sav-05

Summary of our scheme

- Our scheme has **advantages** and may provide some **supplements**
  - **Support for AS relationships.** It considers more major and uncommon AS relationships such as S2S and hybrid relationships, which BAR-SAV has not discussed. It leaves more flexibility for possible new AS relationships.
  - **AS owned address query.** As ROA is not designed for SAV, whether to design specific SAV facilities may need further discussion. If needed, AMS may be retained to provide convenient queries.
  - **Adaptability to changes.** It updates SAV rules actively when changes occur to the networks, no need to wait for notifications after the update from RPKI.
  - **Flexible implementation choice.** The deployment and gradual optimization of RPKI may be a long process. It can flexibly choose various implementations.

Next Step

- Next, we hope to obtain more complex AS relationships and connection scenarios from network operators. Based on these, we will analyze the effects of our SAV scheme in more practical cases and perform targeted optimization on it.

- We will further refine our SAV implementations such as the extension to BGP. In addition, we will optimize them, enhance their security and efficiency, and reduce their overhead to increase the deployment benefits of our SAV scheme.

Thank you!