draft-li-sav-gap-analysis

Source Address Validation: Use Cases and Gap Analysis

Dan Li (Tsinghua University)

Jianping Wu (Tsinghua University)

Mingqing Huang (Huawei)

Lancheng Qin (Tsinghua University)

Nan Geng (Huawei)

SAV is Important and Challenging

□SAV (source address validation) is important

- ◆Source address spoofing leads to various malicious attacks [RFC 6959], represented by reflective DDoS attack
- ◆Network devices deploy SAV to permit traffic with valid source address and block traffic with invalid source address
- ◆Since 2014, the MANRS initiative is calling on network operators to implement SAV as close to the source as possible

□SAV is challenging

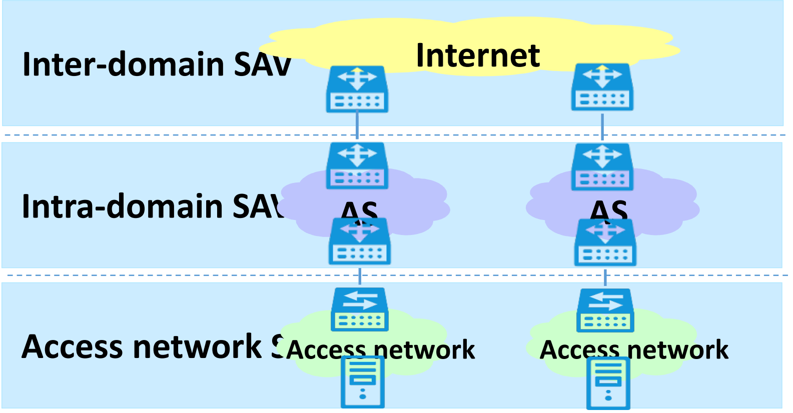
- ◆Accuracy: avoid improper block and reduce improper permit as much as possible
- ◆Incremental deployment: partial deployment can also bring benefit
- ◆Cost: the deployment cost should be affordable

IETF RFCs for SAV Mechanisms

SAV is a problem with long history of attention in IETF

- □Ingress filtering / ACL based SAV [RFC 2267, 2827], Jal 1998 - May 2000
  - ◆Problem: manual configuration
- □Strict-uRPF / Feasible-uRPF [RFC 3704], Mar 2004
  - ◆Problem: improper block under asymmetric routing
- □Feasible-uRPF / Loose-uRPF [RFC 3704], Mar 2004
  - ◆Problem: improper permit
- □SAVI [RFC 6620, 6959, 7039, 7219, 7513, 8074], May 2012 - Feb 2017
  - ◆Host-level SAV in access networks (enterprise networks)
- □EFP(enhanced feasible path)-uRPF [RFC 8704], Feb 2020
  - ◆Mitigating the problem of strict-uRPF / feasible-uRPF in some cases

Necessity of New Intra-/Inter-domain SAV Technologies



□SAVA architecture [RFC 5210] divides SAV into three checking levels

- ◆Access-network SAV, intra-domain SAV, inter-domain SAV

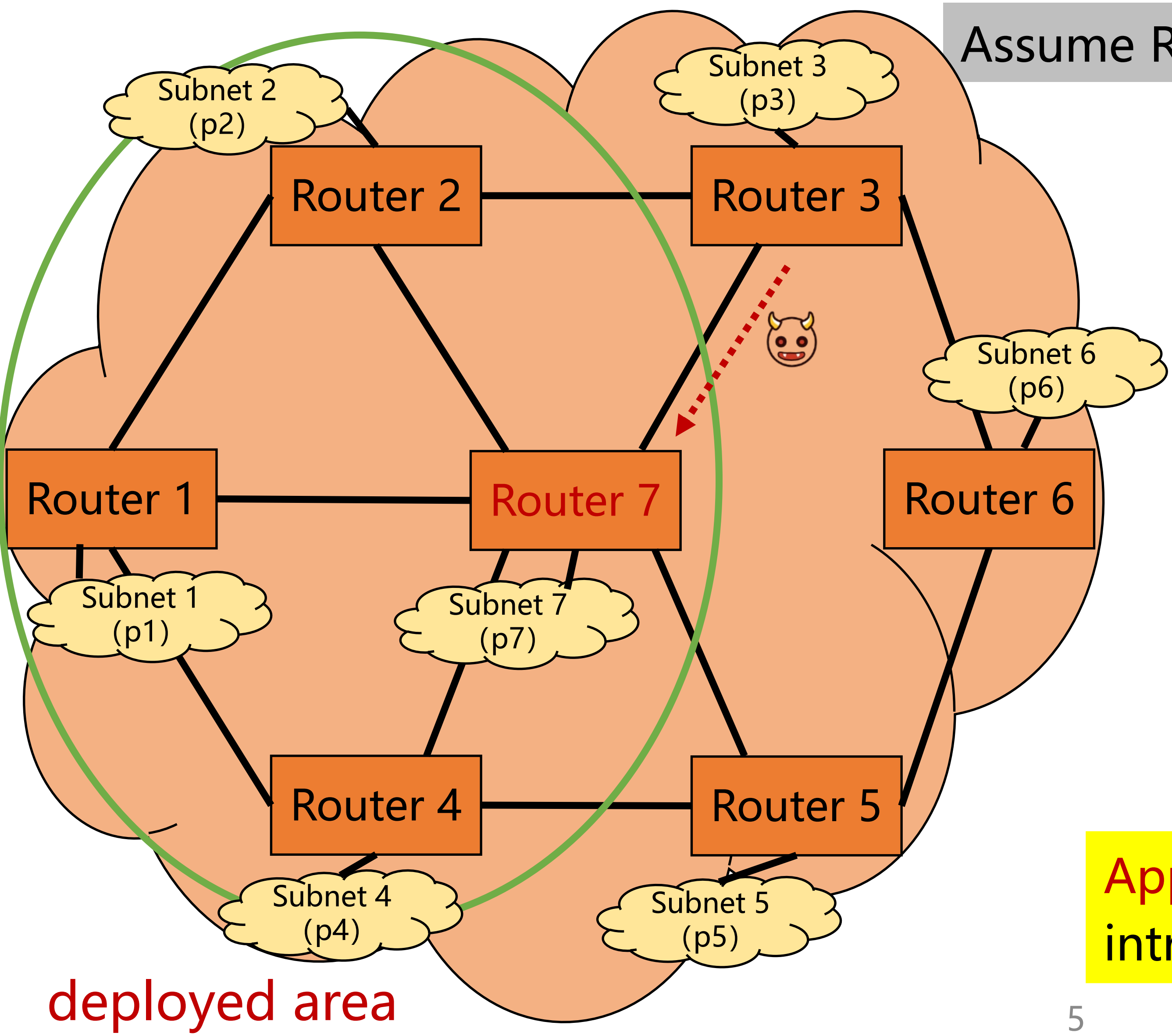
□SAVI for access-network SAV is not enough

- ◆The number of operators for access networks is huge, so it is difficult to require all access networks to deploy SAVI
- ◆When some access networks do not deploy SAVI, intra-domain and inter-domain SAV can help filter spoofing traffic as close to the source as possible

□uRPF-based technology for intra-/inter-domain SAV is not enough

- ◆Strict-uRPF, feasible-uRPF and loose-uRPF have well-known improper block or improper permit problems
- ◆EFP-uRPF does not completely solve the problem

Improper Permit Problem in Intra-domain SAV

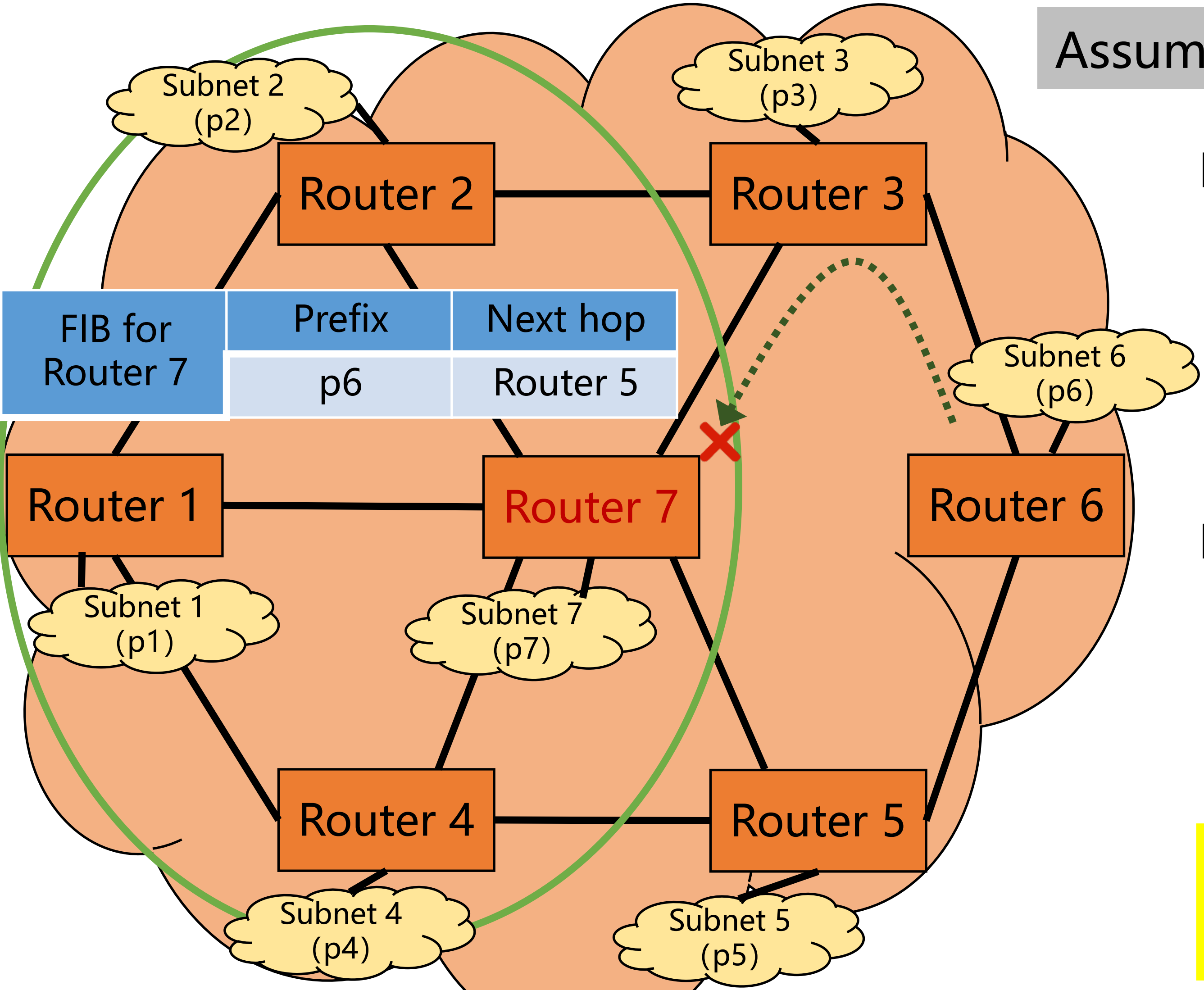


Assume Router 7 applies strict-uRPF only at subnet port

- □ If all the other routers make the same deployment
  - ◆ No problem
- □ If only Router 1,2,4,7 make the same deployment, there will be problem
  - ◆ When Router 3 sends packets to Router 7 by spoofing the source addresses of p1, p2, p4, Router 7 will improperly permit the packets
  - ◆ Subnets in the undeployed area can spoof the source addresses of the deployed area

Applying strict-uRPF only at subnet port in intra-domain SAV has improper permit problem.

Improper Block Problem in Intra-domain SAV



FIB for Router 7	Prefix	Next hop
	p6	Router 5

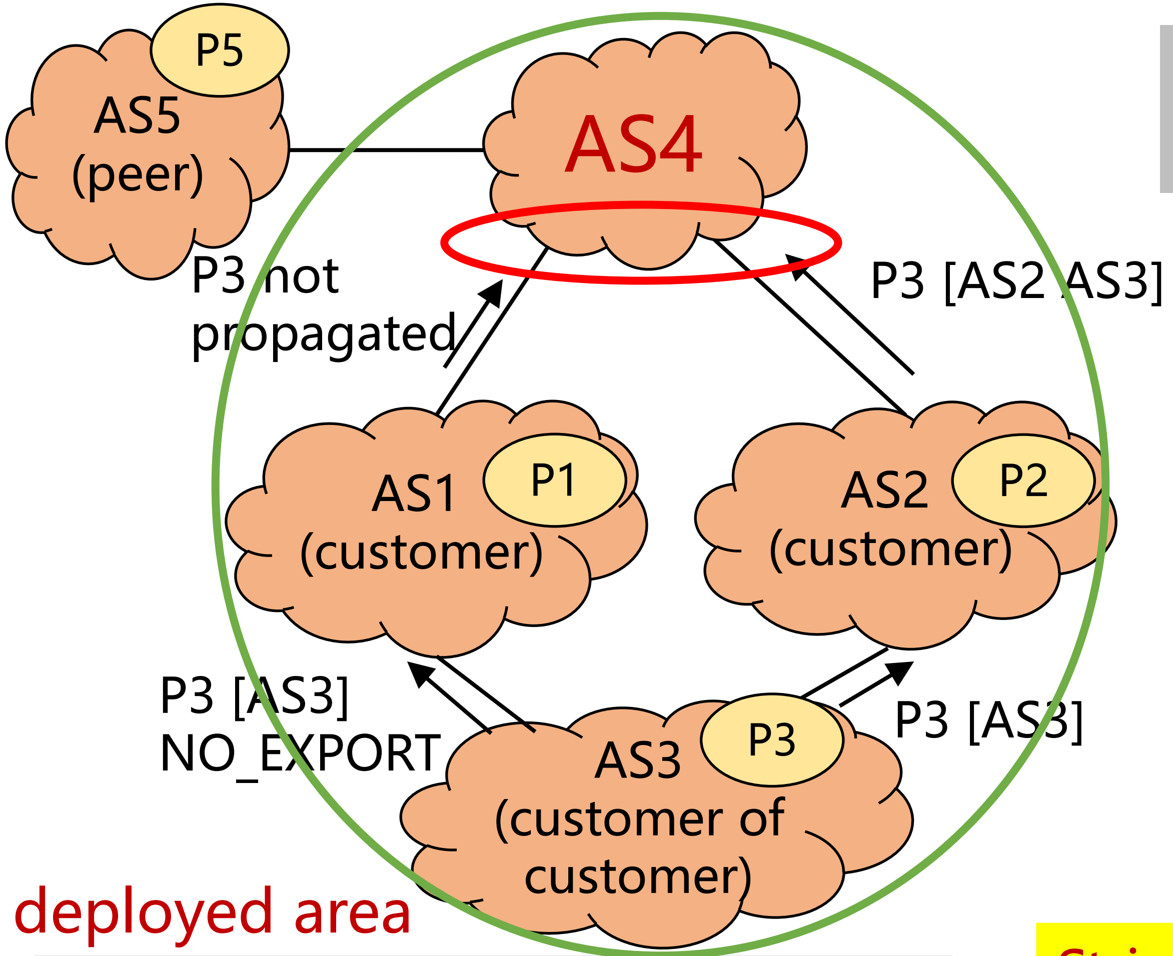
deployed area

Assume Router 7 applies strict-uRPF at all ports

- □ If there is asymmetric routing
  - ◆ The routing path from Router 7 to Router 6 is Router 7 -> Router 5 -> Router 6
  - ◆ The routing path from Router 6 to Router 7 is Router 6 -> Router 3 -> Router 7
- □ The problem
  - ◆ When Router 6 sends valid packets to Router 7 through Router 3, Router 7 will improperly block the packets

Applying strict-uRPF at all ports in intra-domain SAV has improper block problem.

Improper Block Problem in Inter-domain SAV



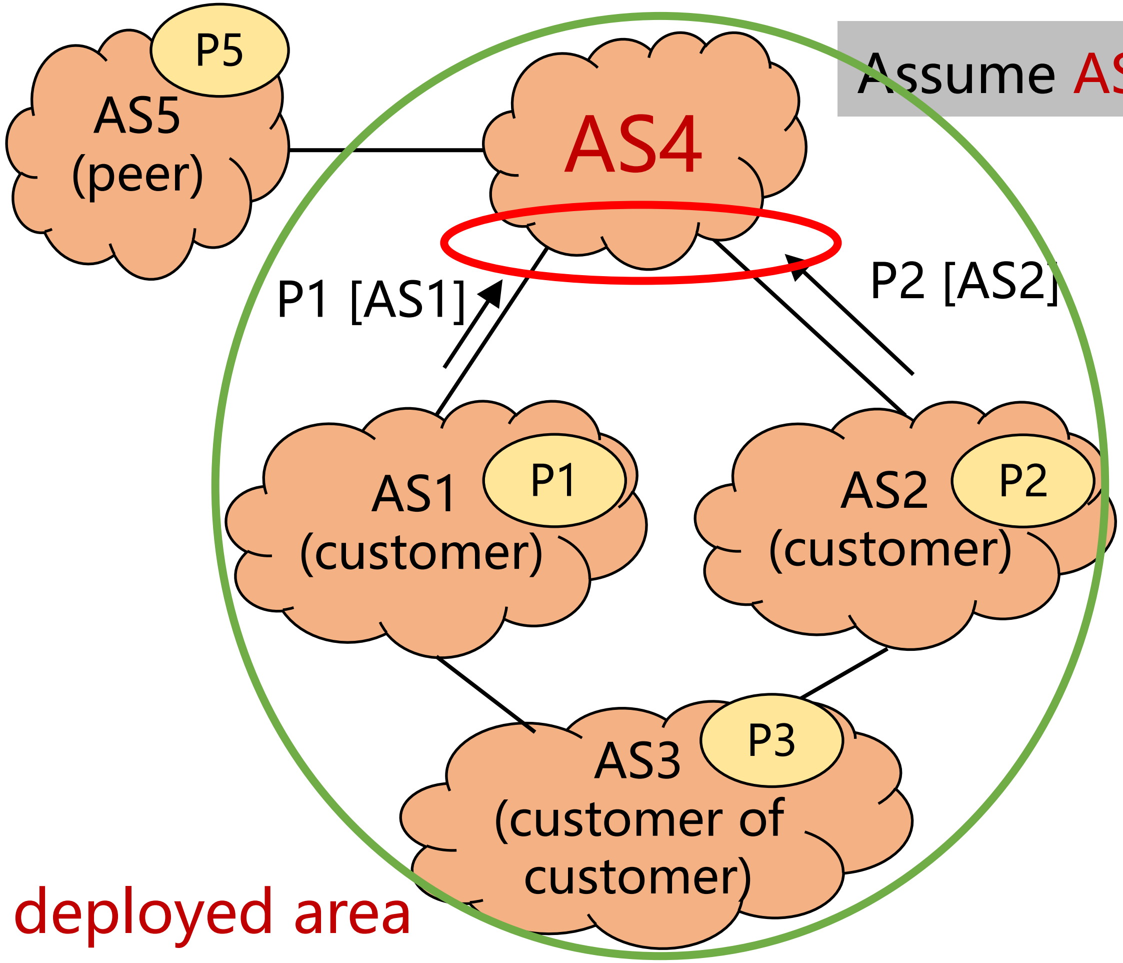
Due to the NO_EXPORT community, route for P3 is not propagated along the path of AS3->AS1->AS4.

Assume AS4 runs strict-uRPF / feasible-uRPF / EFP-uRPF (with Algorithm A) at customer ports

- □ The SAV rule at AS4's customer ports
  - ◆ Packets with source addresses of P3 can only arrive from AS2
- □ The problem
  - ◆ When AS3 sends packets with valid source addresses to AS4 through AS1, AS4 will improperly block these packets

Strict-uRPF / feasible-uRPF / EFP-uRPF (with Algorithm A) in inter-domain SAV has improper block problem.

Improper Permit Problem in Inter-domain SAV



Assume AS4 runs EFP-uRPF (with Algorithm B) at customer ports

- The SAV rule at AS4's customer ports
  - AS4 generates an allowlist containing source prefixes of the customer cone, and applies the allowlist to all customer ports
  - Benefit: packets from AS4's customer cone cannot spoof the source addresses of outside ASes, which is finer-grained than using loose-uRPF
- Problem
  - When packets from AS1, AS2 and AS3 spoof the source addresses of each other, AS4 will improperly permit these packets

AS1 and AS2 advertise their routing information to AS4 through BGP

Loose-uRPF / EFP-uRPF (with Algorithm B) in inter-domain SAV has improper permit problem.

The Root Cause of uRPF's Inaccuracy Problem

- The root cause of the improper block and improper permit problem for uRPF-based SAV mechanisms
  - They all leverage the local FIB/RIB table of routers to decide the incoming interface of packets, which may not match the real data-plane forwarding path
- To achieve accurate SAV
  - A network-level protocol is required to build an independent and accurate SAV table in each router, which follows the real data-plane forwarding path
  - Compared with strict-uRPF, the SAV table is different from the FIB table, so the improper block problem under routing asymmetry can be avoided
  - Compared with feasible-uRPF/loose-uRPF/EFP-uRPF, the SAV table is finer-grained, so the improper permit problem can be avoided

Requirements of Network-level SAV Protocol

- □ Basic requirement
  - ◆ High accuracy: avoid improper block & reduce improper permit as much as possible
- □ Other requirements
  - ◆ High scalability: the protocol should not cause too much computation and communication overhead
  - ◆ Incremental deployment: when partial routers in an AS or partial ASes in the Internet deploy the new protocol, there will be obvious gain compared with uRPF-based SAV
  - ◆ High security: the security and integrity of the protocol messages should be guaranteed
- □ Basic idea of our solution to satisfy all the requirements above
  - ◆Discovering the real data-plane forwarding path via hop-by-hop prefix notification, and generating SAV tables in routers along the path

Summary

- □Intra-domain and inter-domain SAV is an important and unsolved problem in our community
- □In both intra-domain and inter-domain scenarios, uRPF-based SAV mechanisms have either improper block problem or improper permit problem
- □The root cause of uRPF-based SAV is the dependence on router’s local FIB/RIB
- □To achieve accurate SAV, a network-level protocol is required to build an independent and accurate SAV table in each router, which follows the real data-plane forwarding path

Thanks!