Intra-domain Source Address Validation (SAVNET) Architecture

Dan Li, Jianping Wu, **Lancheng Qin,** Nan Geng, Li Chen,
Mingqing Huang, Fang Gao

November 8, 2023

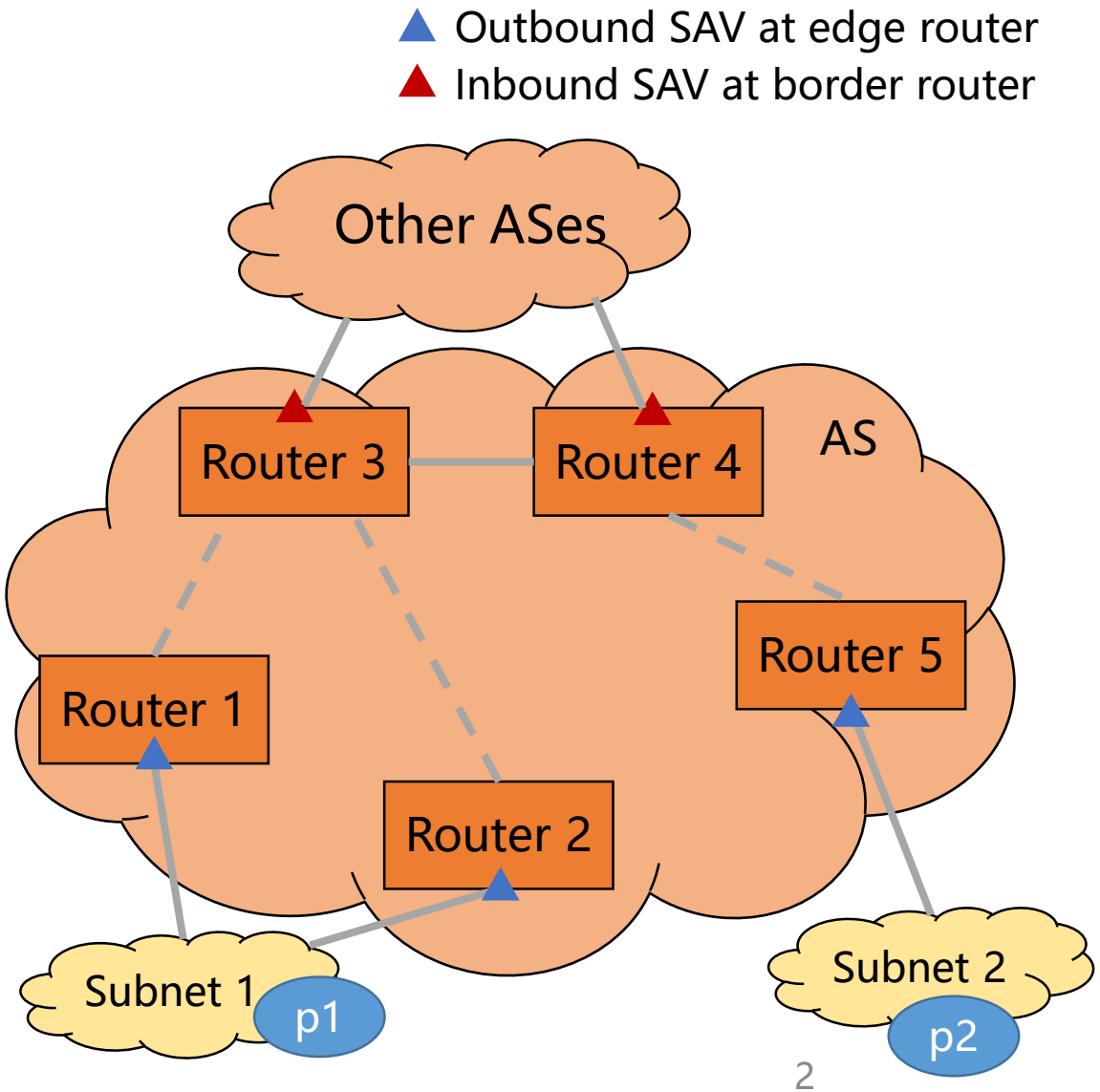
Two Goals of Intra-domain SAV

Goal #1: Outbound traffic validation

- **Edge routers** should block illegitimate packets **coming from the AS's intra-domain subnets** which **forge source addresses of other subnets** (either within the AS or other ASes)

Goal #2: Inbound traffic validation

- **Border routers** should block illegitimate packets **coming from other ASes** which **forge internal source addresses**



Review of Intra-domain SAV Problem Statement

- Problems of existing intra-domain SAV mechanisms[1]
  - ACL-based SAV requires high operational overhead
  - uRPF-based SAV has improper block or improper permit problems
- Requirements of the new intra-domain SAV mechanism[1]
  - Automatic update
  - Accurate validation
  - Incremental/partial deployment
  - Convergence
  - Security

[1]: draft-ieft-savnet-intra-domain-problem-statement-02

Background of Intra-domain SAVNET Architecture

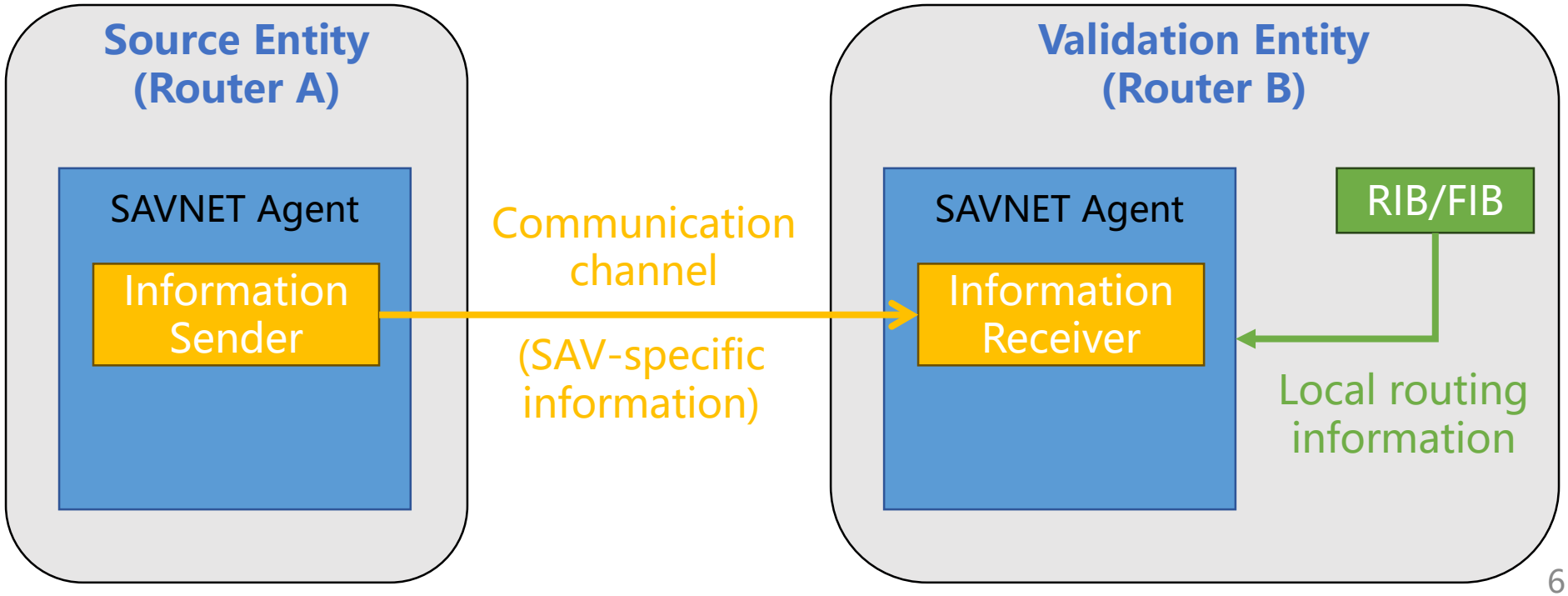
- Intra-domain SAVNET architecture aims to achieve accurate SAV in an intra-domain network by an automatic way
  - Address the problems of existing intra-domain SAV mechanisms
  - Meet the requirements proposed in [draft-ietf-savnet-intra-domain-problem-statement]
- Historical versions
  - draft-li-savnet-intra-domain-architecture-00, IETF 115 SAVNET WG
  - draft-li-savnet-intra-domain-architecture-01, IETF 116 SAVNET WG
  - draft-li-savnet-intra-domain-architecture-02, June 1, 2023
  - **draft-li-savnet-intra-domain-architecture-03, IETF 117 SAVNET WG**
  - draft-li-savnet-intra-domain-architecture-04, Oct. 20, 2023
  - **draft-li-savnet-intra-domain-architecture-05, IETF 118 SAVNET WG**

Main Updates Compared to Version-03

- Updates in Intra-domain SAVNET Architecture section
  - Clarify the content of SAV-specific information
  - Introduce the SAV rule generation process for edge router and border router, respectively
- Updates in Use Cases section
  - Use the two use cases proposed in [draft-ietf-savnet-intra-domain-problem-statement] to illustrate intra-domain SAVNET achieves more accurate and efficient SAV than existing intra-domain SAV mechanisms
- Add a new section
  - Describe how intra-domain SAVNET meet the five design requirements proposed in [draft-ietf-savnet-intra-domain-problem-statement]

Key Idea of Intra-domain SAVNET Architecture

- Exchange SAV-specific information among routers automatically
- Generate SAV rules in routers based on both SAV-specific information and local routing information

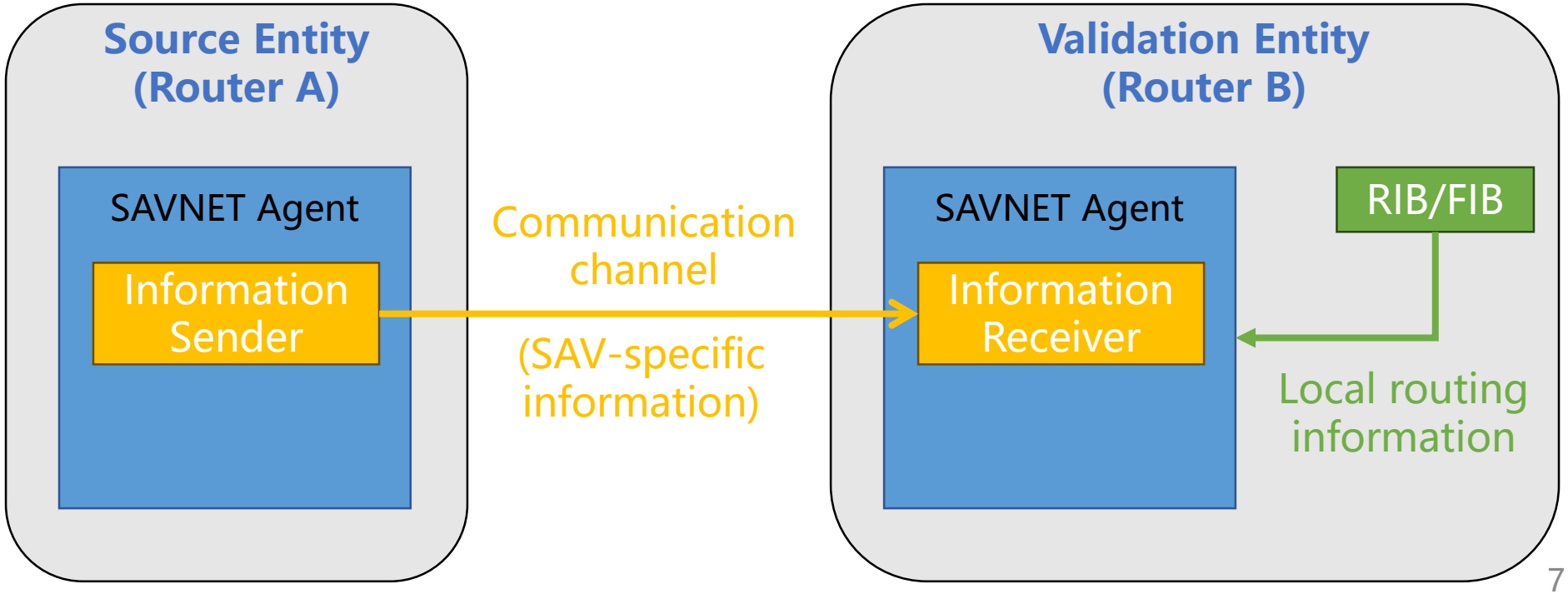


Source Entity and Validation Entity

An intra-domain router can act as one or two roles: source entity or/and validation entity

Source entity sends its SAV-specific information to other routers

Validation entity receives SAV-specific information from other routers and generates SAV rules based on SAV-related information

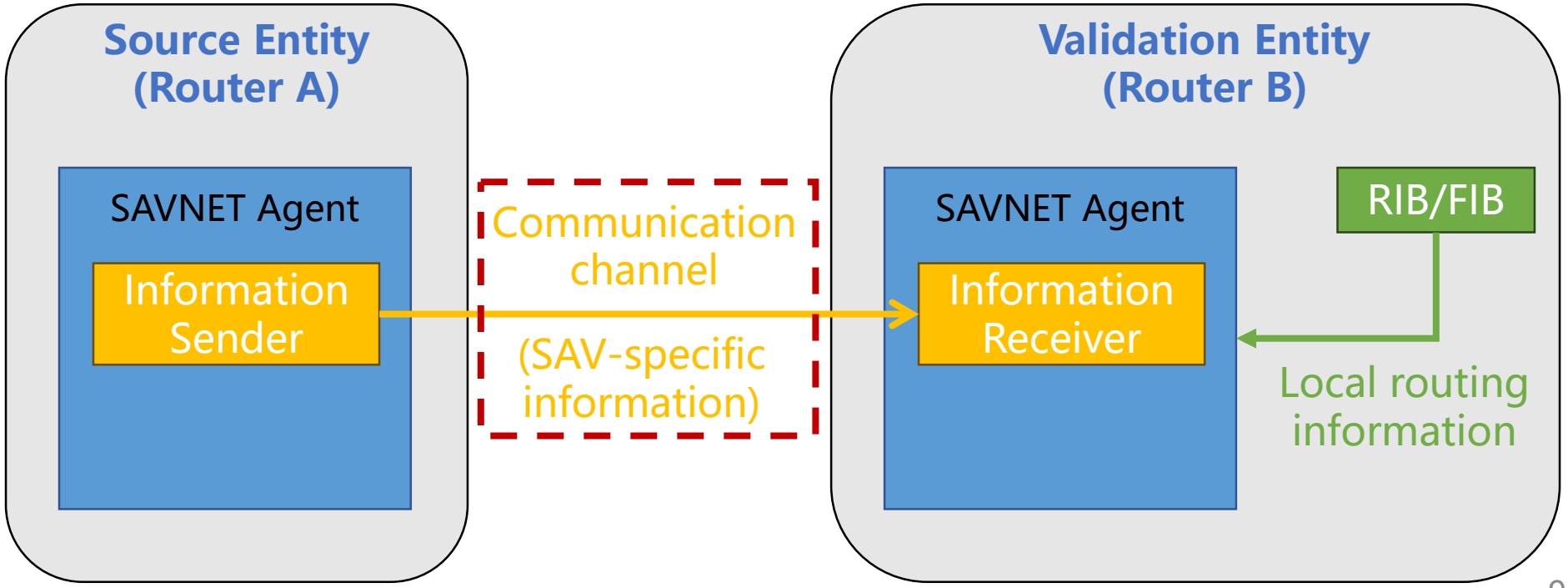


SAV-specific Information

- SAV-specific information is specialized for SAV rule generation
  - It carries necessary information which cannot be learned from local routing information in asymmetric routing scenarios, helping generate accurate SAV rules
- Examples of SAV-specific information in intra-domain SAVNET
  - The router's locally known source prefixes of its connected subnets
  - The ownership of source prefixes, e.g., belonging to a single-homed subnet or belonging to a multi-homed subnet
  - The type of source prefixes, e.g., anycast prefix, hidden prefix, etc.
- A new mechanism (namely, SAV-specific information communication mechanism) is needed to communicate SAV-specific information

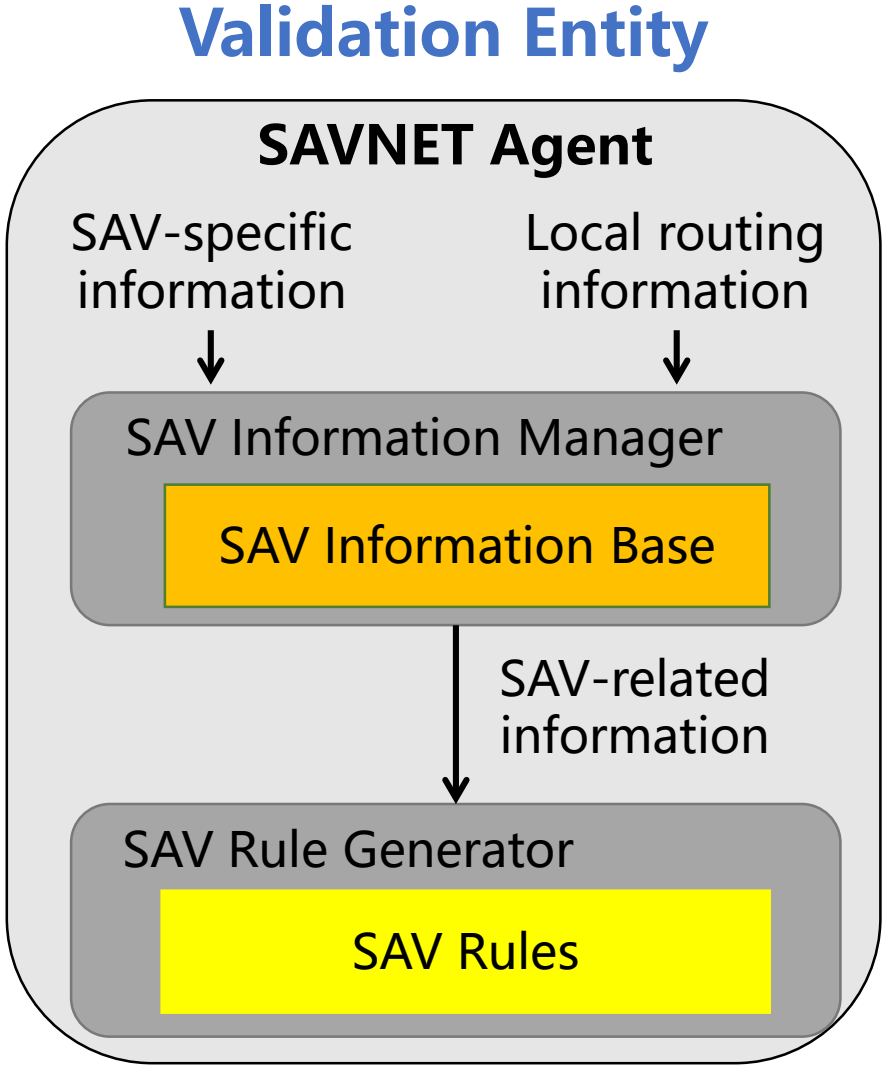
SAV-specific Information Communication Mechanism

- Building the communication channel and propagating SAV-specific information from source entity to validation entity
  - Automatic update in a timely manner
  - Session authentication before session establishment



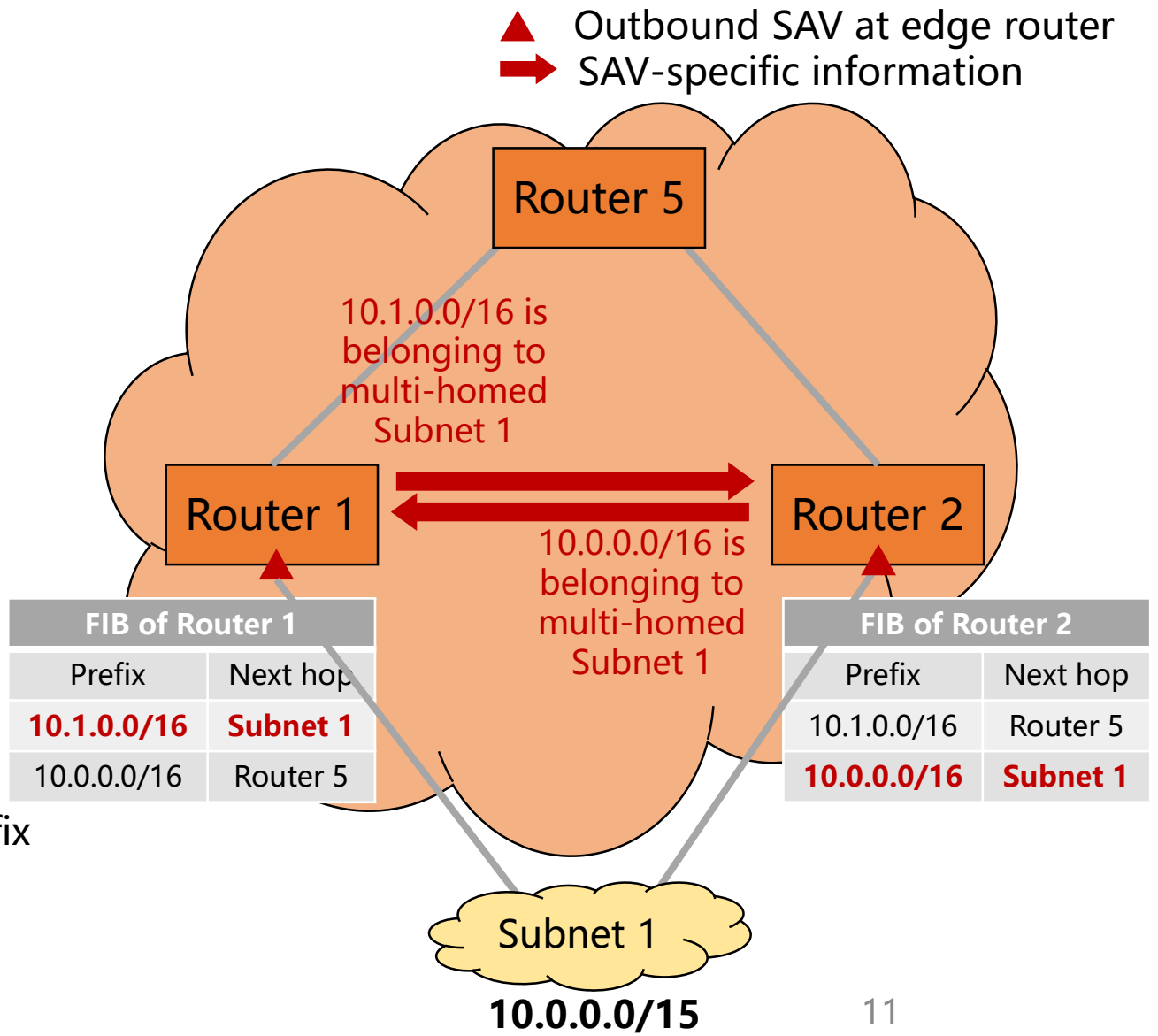
SAV Rule Generation

- Edge routers generate SAV rules and perform outbound SAV
  - ◆Obtain the complete source prefixes of each connected subnet based on SAV-specific information and local routing information
- Border routers generate SAV rules and perform inbound SAV
  - ◆Obtain internal source prefixes of the AS based on SAV-specific information and local routing information



Use Case #1: Outbound SAV at Edge Routers

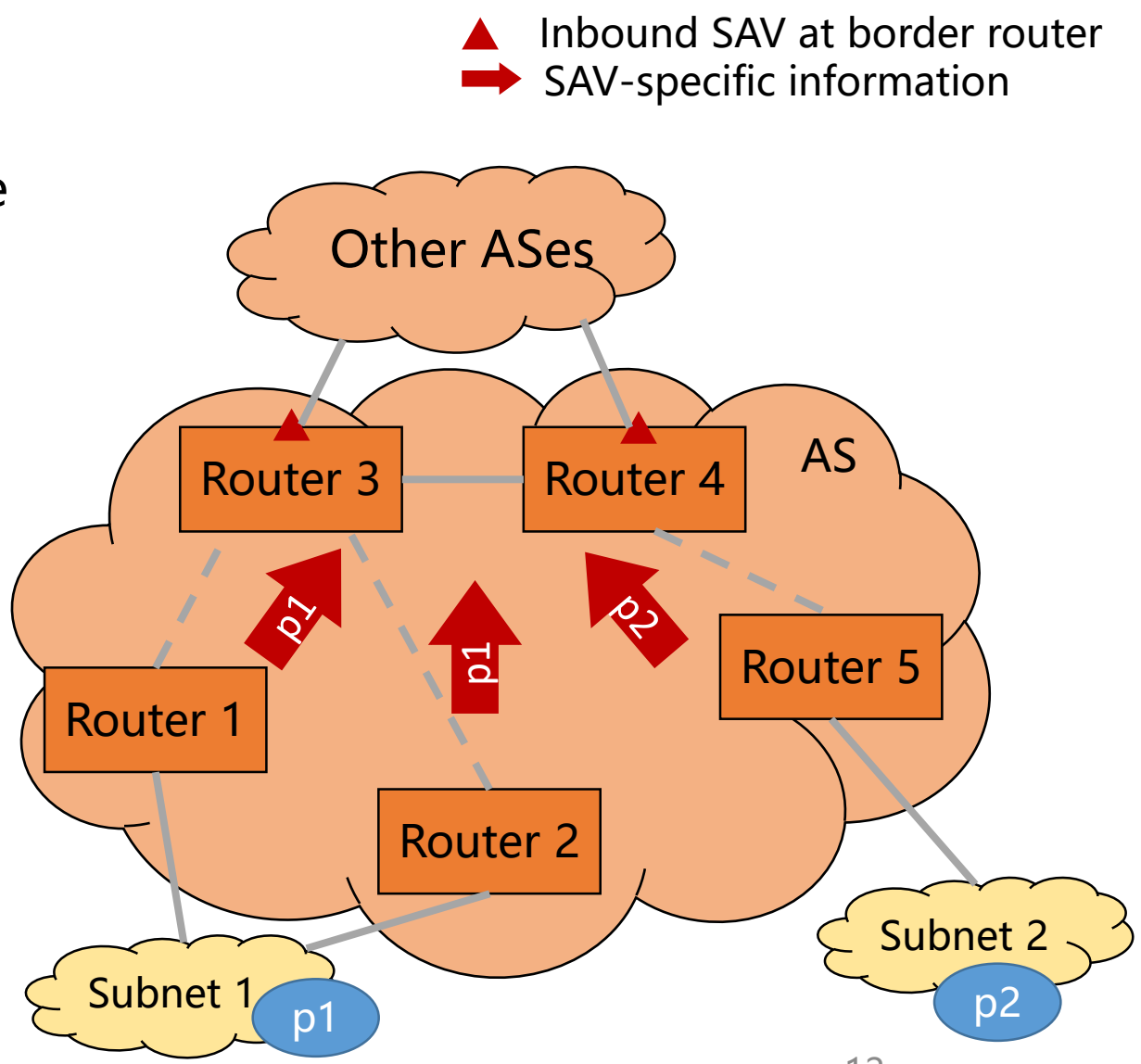
- **Outbound traffic validation in asymmetric routing scenario[1]**
  - Edge routers 1 and 2 only learn part of source prefixes of Subnet 1 from local routing information in the asymmetric routing scenario
- If using strict uRPF
  - Improper block
- If using intra-domain SAVNET
  - **Accurate & Automatic outbound SAV**
    - Routers 1 and 2 obtain the complete source prefix of Subnet 1 by exchanging their locally known source prefixes of Subnet 1



[1]: draft-ieft-savnet-intra-domain-problem-statement-02

Use Case #2: Inbound SAV at Border Routers

- **Inbound traffic validation[1]**
  - Border routers 3 and 4 should block inbound packets with source address of internal source prefixes at border routers
- If using ACL-based SAV
  - Manual update when internal prefixes or network topology change dynamically
- If using loose uRPF
  - Large amount of improper permit
- If using intra-domain SAVNET
  - **Accurate & Automatic inbound SAV**
    - Routers 3 and 4 obtain the complete internal source prefix based on SAV-specific information sent by Routers 1, 2, and 5



[1]: draft-ieft-savnet-intra-domain-problem-statement-02

Accurate Validation & Automatic Update

Use Cases #1 and #2 shows that intra-domain SAVNET can **achieve more accurate validation and support automatic update**

- Compared with uRPF-based SAV which solely uses local routing information,
  - Intra-domain SAVNET generates SAV rules by using both local routing information and SAV-specific information exchanged among routers, resulting in more accurate SAV validation in asymmetric routing scenarios
- Compared with ACL-based SAV which requires manual updates,
  - Intra-domain SAVNET generates SAV rules automatically in a distributed way and allows routers to exchange the changes of SAV-specific information among each other automatically

Incremental/Partial Deployment

- Edge routers and border routers deploying intra-domain SAVNET is enough
- Blocking spoofing traffic in incremental/partial deployment scenarios
  - Outbound SAV: as long as edge routers connected to the same subnet exchange SAV-specific information, that subnet can be accurately prevented from spoofing other subnets
  - Inbound SAV: if a border router only obtains partial internal source prefixes, it can still block inbound packets which forge those prefixes
  - When SAV-specific information is missing, local routing information can be used to generate SAV rules
- More routers deploy intra-domain SAVNET, more benefits

Convergence

- When SAV-related information changes,
  - Source entity MUST send the updated SAV-specific information to validation entity **timely**
  - Validation entity MUST detect the changes of received SAV-specific information and local routing information in time and update SAV rules with the latest information
- Propagation speed of SAV-specific information is the main factor that affects the convergence of SAV rule generation
  - SAV-specific information can have a similar propagation speed as routing information
    - if SAV-specific information and routing information of an edge router can be advertised to other routers in a similar way
  - Depending on the design and implementation of the new intra-domain SAV solution

Security

- In some unlikely cases, some routers may do harm to other routers within the same domain
  - Potential threats: entity impersonating, message blocking, message alteration, message replay, etc.
- The above security threats SHOULD be considered when designing the new intra-domain SAV mechanism
  - Possible solutions: session authentication, message acknowledge, message integrity verification, duplication detection, etc.

Summary

Following this architecture, the new SAV solution can meet the requirements proposed in [draft-ieft-savnet-intra-domain-problem-statement]

- Requirement #1: Accurate Validation
  - Generate SAV rules using both SAV-specific information and local routing information
- Requirement #2: Automatic update
  - SAV-specific information exchange is triggered automatically when topology or prefix changes
- Requirement #3: Incremental/partial Deployment
  - When some SAV-specific information is unavailable, local routing information can be used to fill this gap
- Requirement #4: Convergence
  - SAV-specific information and SAV rules can be updated in a timely manner
- Requirement #5: Security
  - Possible security threats should be considered when designing the new SAV solution

Thanks!