IETF 118 SAVNET WG

Emulations of 9 SAV Mechanisms with SAV Open Playground

Libin Liu, **Li Chen**
Zhongguancun Laboratory

SAVNET WG Meeting, IETF 118
November 8, 2023

Motivation

It remains a significant challenge to promote the wide deployment of SAV

Lack of understanding

- Many people lack the technical knowledge, understanding, and practical experience. They do not know how SAV works or how to deploy or operate a specific SAV mechanism.

Lack of open source implementation

- There is very limited open source effort on SAV, it is difficult to form an acknowledged baseline standard, leading to differences in understanding and implementation of the same SAV mechanism.

Performance concerns

- People cannot test and evaluate the performance of different SAV mechanisms, due to the lack of a publicly available testbed. Without sufficient tests, network operators hesitate to deploy SAV mechanisms in their networks.

Motivation

It remains a significant challenge to promote the wide deployment of SAV

Lack of understanding

- Many people lack the technical knowledge, understanding, and practical experience. They do not know how SAV works or how to deploy or operate a specific SAV mechanism.

SAVOP provides an open platform to implement and emulate different SAV mechanisms.

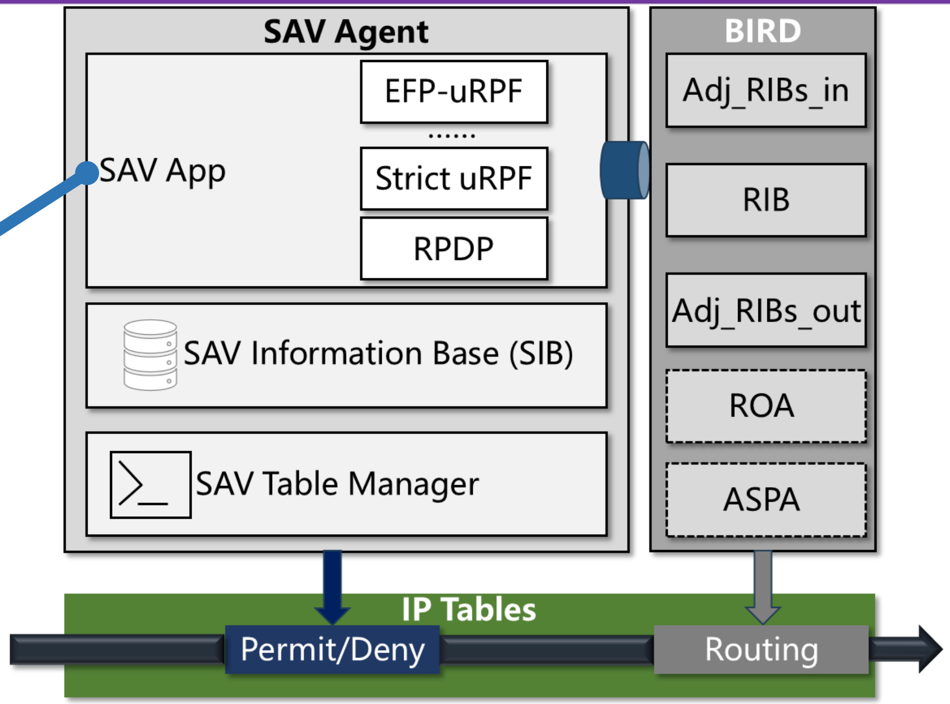
baseline standard, leading to differences in understanding and implementation of the same SAV mechanism.

Performance concerns

- People cannot test and evaluate the performance of different SAV mechanisms, due to the lack of a publicly available testbed. Without sufficient tests, network operators hesitate to deploy SAV mechanisms in their networks.

Nine SAV Mechanisms

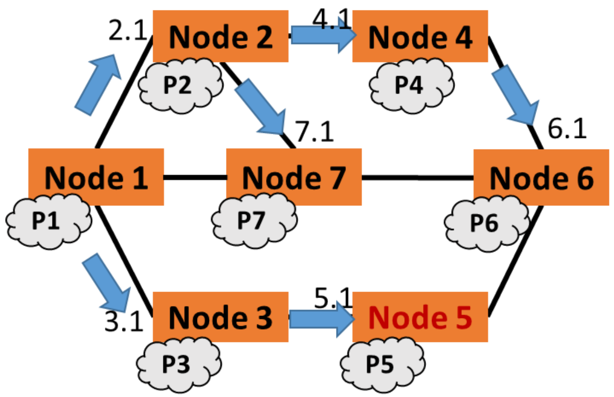
- Loose uRPF[1]
- Strict uRPF[1]
- FP-uRPF[1]
- EFP-uRPF-A[2]
- EFP-uRPF-B[2]
- BAR-SAV[3]
- Passport[4]
- DSAV[5]
- Enhanced DSAV



[1]RFC3704: https://datatracker.ietf.org/doc/html/rfc3704
[2]RFC8704: https://datatracker.ietf.org/doc/html/rfc8704
[3]https://datatracker.ietf.org/doc/draft-ietf-sidrops-bar-sav/
[4]Passport: Secure and Adoptable Source Authentication, NSDI 2008
[5]https://datatracker.ietf.org/meeting/113/materials/slides-113-savnet-dsav-framework-01

DSAV and E-DSAV

- DSAV features hop-by-hop propagation of SAV-specific information, so that the source information will propagate through all possible forwarding paths originated from the source.
  - https://datatracker.ietf.org/meeting/113/materials/slides-113-savnet-dsav-framework-01



- Enhanced DSAV (E-DSAV) makes the three improvements upon DSAV.
  - **Decouple control and data channels**
    - Only the control channel reuses the BGP connection of the underlying router. Exchanges control messages of DSAV (neighbor discovery, data channel context exchange and conncetion setup)
    - For ASNs, the E-DSAV uses a separate data channel (a direct QUIC connection between SAV Agents).
  - ***Use ASN* to replace source prefixes** of the corresponding AS within the communicated messages to further reduce bandwidth requirements.
  - Design a **neighbor discovery mechanism** for building neighbor relationships

Emulation Setups

- **Testbed**
  - Using a x86 server machine with two 2.2GHz 26-core Intel Xeon Gold 5320 CPUs, 256GB DDR4 RAM, 2 1TB SSDs, and 1 12TB SAS HDDs
  - Running Ubuntu 22.04.2 LTS with kernel version 5.15.0
  - Using Docker 24.0.2 with the image ubuntu:22.04 for each container to emulate an AS
  - Running BIRD 2.0.12 as the AS border router and using iptables 1.8.7 to filter packets
- **Methodology**
  - Evaluating the performance of these mechanisms in terms of **validation accuracy, control plane performance, data plane performance, and scalability**
  - Using the network topology with 50 ASes
    - Except for the scalability experiments
  - Varying the deployment ratios of the SAV mechanisms from 10% to 100%

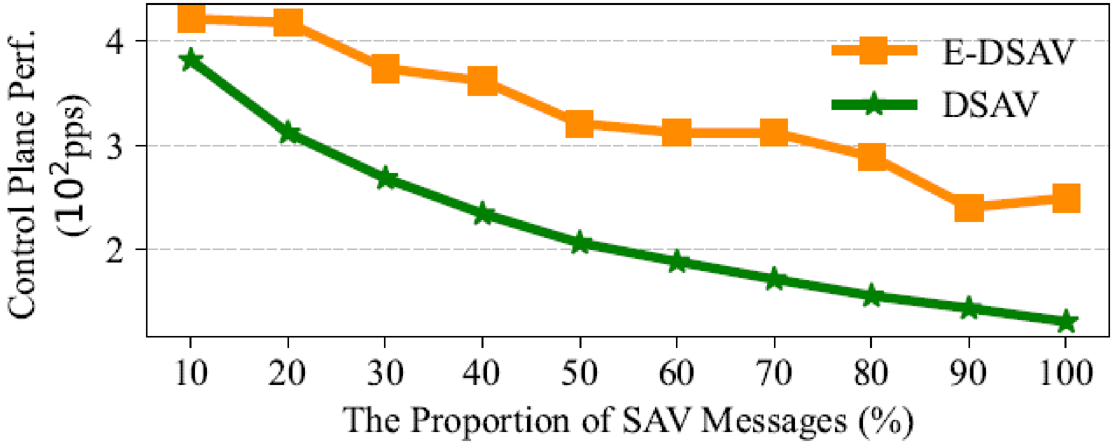
SAV Accuracy

Scenarios	Loose uRPF	Strict uRPF	FP-uRPF	EFP-uRPF-A	EFP-uRPF-B	BAR-SAV	Passport	DSAV	E-DSAV
Symmetric Routing	IP	√	√	√	IP	√	√	√	√
NO-EXPORT	IP	IB	IB	IB	IP	IB	√	√	√
DSR	IP	IB	IB	IB	IP & IB	IB	√	√	√

The SAV accuracy of different SAV mechanisms implemented on top of SAVOP in the scenarios including symmetric routing, NO-EXPORT, and Direct Server Return (DSR) (√: Accurate Validation, IP: Improper Permit, IB: Improper Block).

- Results confirms the theoretical analysis in [draft-ietf-savnet-inter-domain-problem-statement].
  - ◆ In symmetric routing scenario, both Loose uRPF and EFP-uRPF with algorithm B may improperly permit spoofing traffic.
  - ◆ In NO-EXPORT and DSR scenarios, both Loose uRPF and EFP-uRPF with algorithm B may improperly permit spoofing traffic; Strict uRPF, FP-uRPF, EFP-uRPF with algorithm A and B, and BAR-SAV may improperly block legitimate traffic.

Control Plane Performance



- The control plane performance for processing pure BGP messages in terms of packets per second with varying proportions of SAV messages.
- The proportions of SAV messages are calculated by the number of SAV messages over the total number of messages of BGP.

□Both DSAV and E-DSAV reduces the throughput of the BGP routing process.

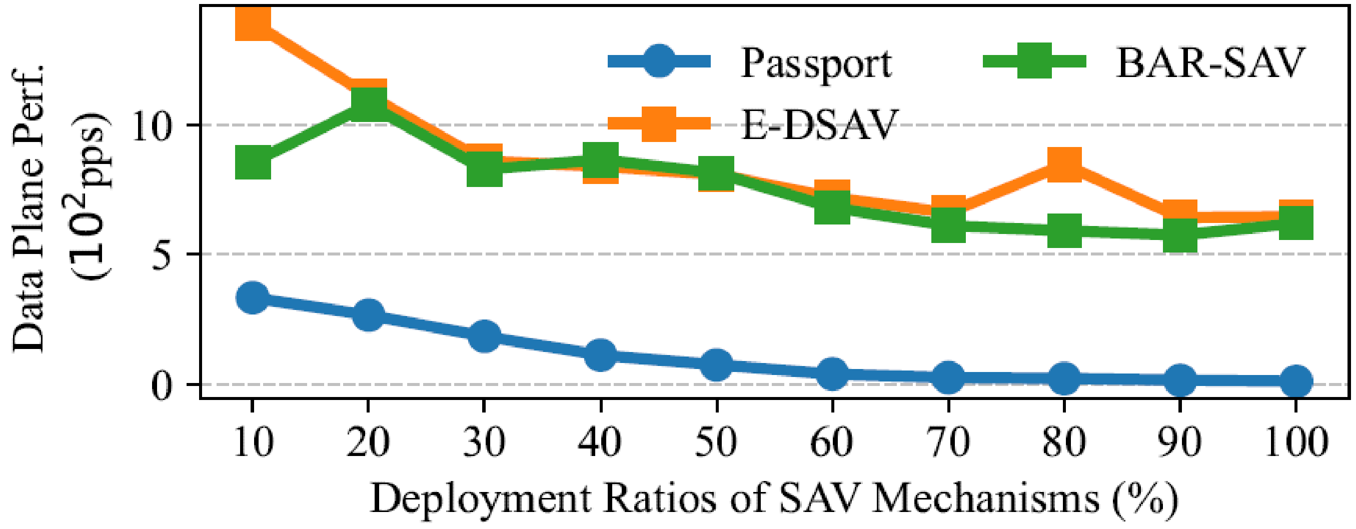
◆ For E-DSAV, the limitations arise from computational and memory constraints within each container. But 53% faster than DSAV.

◆ DSAV not only needs to communicates more messages but also necessitates **additional resources for parsing** the delivered SAV messages that contains SAV-Specific information.

➢Because control and data are using the same communication channel.

◆ Proposing a **design principle for SAVNET**: We SHOULD limit the negative impact of SAVNET on underlying routing protocol instances.

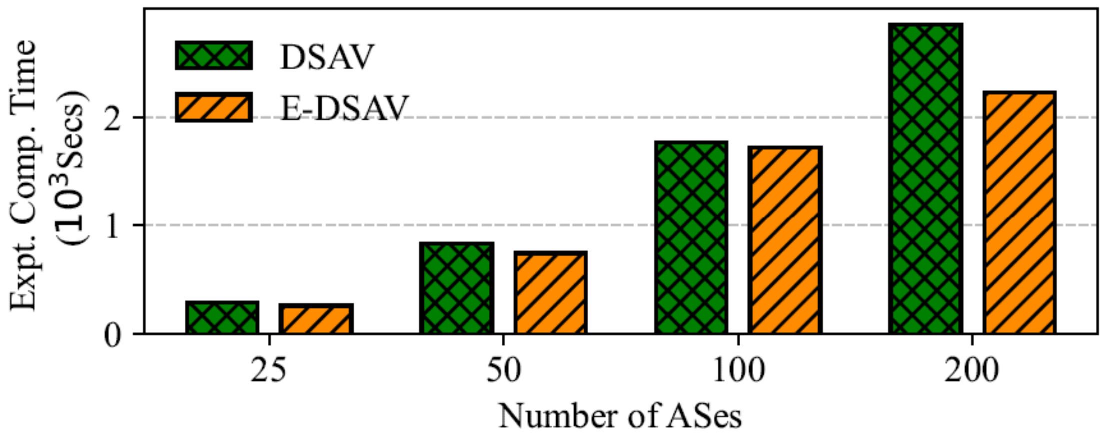
Data Plane Performance



- The data plane forwarding performance of the SAV mechanisms with varying deployment ratios.
- We employ iptables to execute SAV within the data plane.
- We implement a traffic generation tool to generate packets with fixed 1.5KB to evaluate the data plane forwarding performance in terms of packets per second.

- Passport performs significantly worse, because cryptographical SAV requires the router to perform **cryptographic computation** on each packet, which increases the processing overhead **(>500x slow down).**
- The data plane forwarding performance of each SAV mechanism decreases as the deployment ratio increases.
  - This is because the **size of the SAV table** within each AS increases with **the increase of deployment ratio**, larger SAV table results in longer query time for each incoming packet.

Scalability of SAVOP



- The experiment completion time of SAVOP across different network scales.
- We vary the network scales by increasing the number of ASes for the testbed experiments, and then calculate the experiment completion time.
- The experiment completion time is the longest time elapsed from launching the Docker environment to generating complete SAV Table among all ASes.

- The figure shows the total experiment time of SAVOP with AS numbers from 25 to 200, by taking DSAV and E-DSAV as examples.
  - **A server with 256GB DDR4 RAM can run 200 SAVOP containers** with our current implementation
  - E-DSAV with a 200-AS network topology converges within ~47 minutes.
    - Limited by compute and memory.
  - Compared with DSAV, E-DSAV shows a slower growth trend with the increase of network size. This is because E-DSAV converges faster than DSAV.

Summary

SAVOP continues to help the completion of WG Charter items.

SAVOP

- Implement and emulate the uRPF-based SAV mechanisms in different network scenarios, and analyze the emulation results
- Implement and emulate a new SAV mechanism called E-DSAV, which is implemented by extending BGP, and demonstrate its accuracy improvement upon existing mechanisms
- Plan to implement new mechanisms for generating SAV rules by extending BGP and emulate them in various network scenarios

Charter of SAVNET WG

...existing SAV mechanisms like uRPF-related technologies may improperly permit spoofed traffic or block legitimate traffic...

...should include an analysis of the current solutions and their limitations...

...The accuracy of the new SAV mechanisms is expected to improve upon the current ones...

...The SAVNET WG will coordinate and collaborate with other WGs as needed. Specific interactions may include (but are not limited to): idr for BGP extensions...

Thanks! ☺

https://github.com/SAV-Open-Playground

SAV Benchmark

- Real-world AS-level network topology
  - Using real BGP data from public route collectors provided by RouteViews[1] and RIPE RIS[2]
  - Parsing and extracting *AS path* attribute from the BGP data and obtaining neighboring relation between ASes
  - Creating links for the neighboring ASes to build the AS-level Internet topology
  - Obtaining the business relationship between ASes according to the data from CAIDA[3]
- Sub-graphs generated based on the full topology
  - A connected component of the full topology
  - Assigning routing policies based on the business relationship and the valley-free principle
- Three classic scenarios
  - Symmetric routing, NO_EXPORT, direct server return (DSR)

[1]http://www.routeviews.org/routeviews/
[2]https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data
[3]https://catalog.caida.org/dataset/as_relationships_serial_1