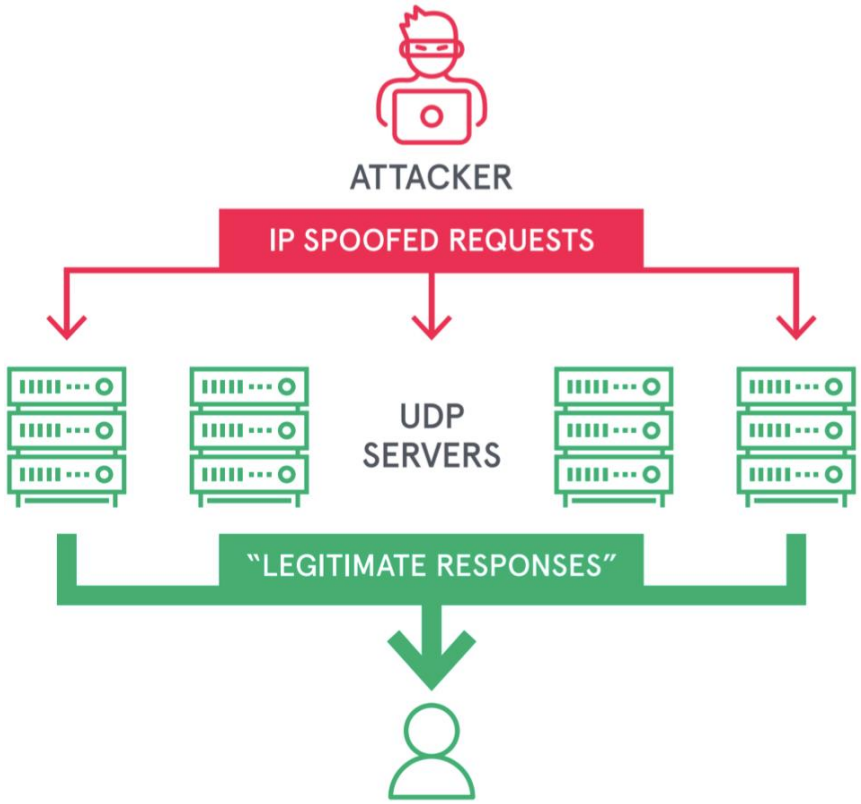
pSAV: A Practical and Decentralized Inter-AS Source Address Validation Service Framework

Jiamin Cao, Ying Liu, Mingxing Liu, Lin He, Yihao Jia, Fei Yang

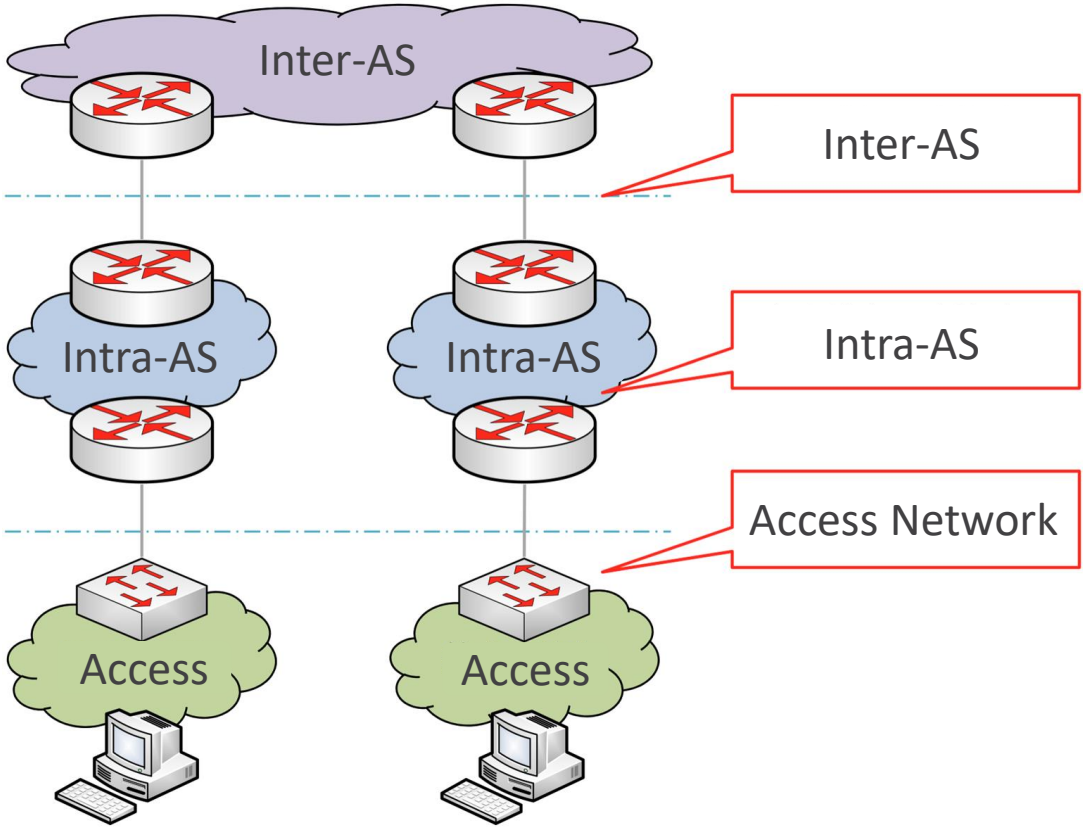
Source IP Spoofing

- **Large attacks use source IP spoofing**
  - Attackers hide their identities
  - Attack traffic is amplified with reflection
- **Why source IP addresses can be spoofed?**
  - Routing is based on destination IP addresses, without validating source addresses



Source Address Validation Architecture (SAVA)

- **Source address validation (SAV) in three levels**



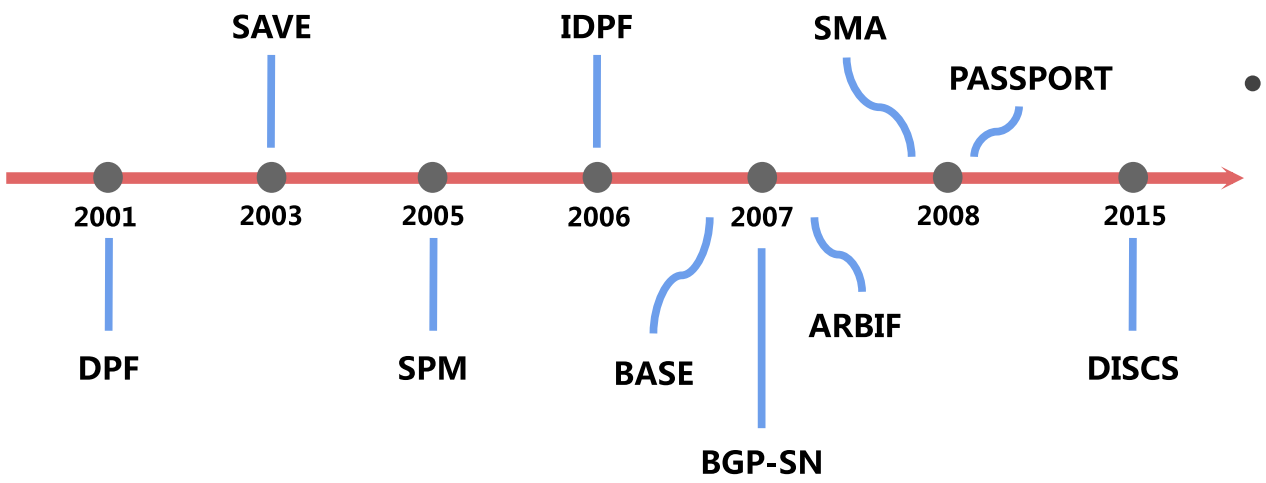
RFC5210 SAVA

Defend against IP spoofing attacks from outside.

Benefit the entire Internet, except for the deployers themselves.

Inter-AS SAV faces deployment challenges

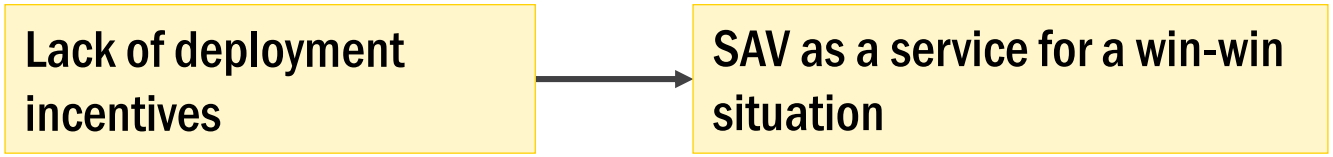
The development of inter-AS SAV technologies



- The benefits are obvious, but why is there less and less research?

Inter-AS SAV faces deployment challenges

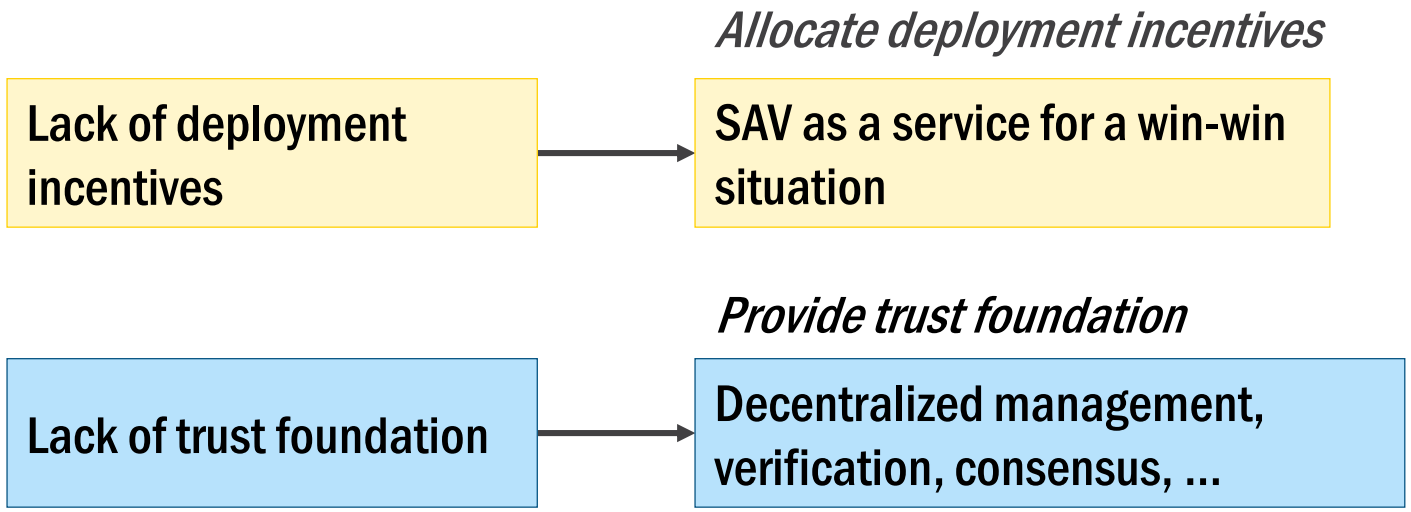
Allocate deployment incentives



Lack of deployment incentives: the efforts and benefits do not match

- In a security alliance, ASes at the alliance boundary naturally have to bear more of the burden of inspecting packets and have less incentive to deploy SAV.

Inter-AS SAV faces deployment challenges

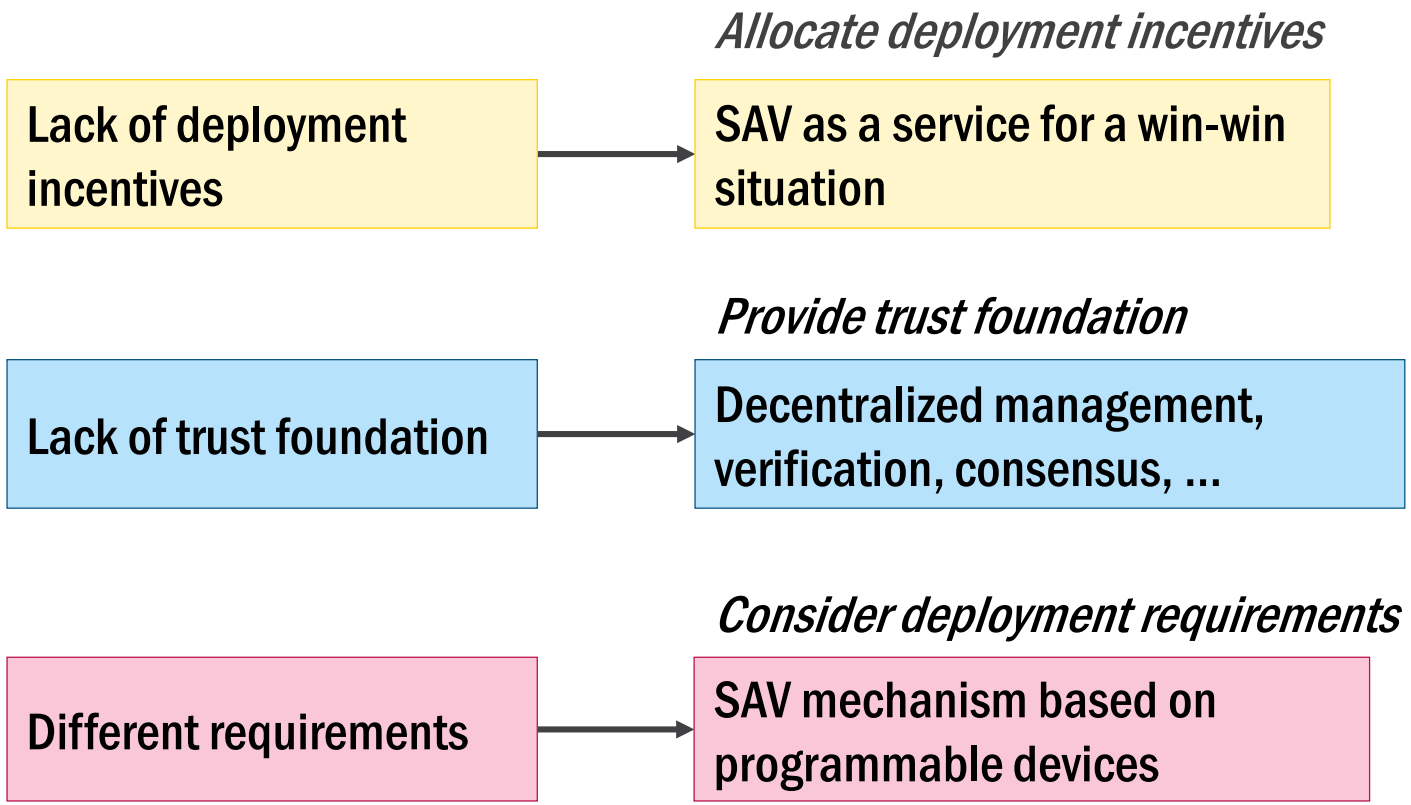


Lack of trust foundation

- Allow spoofed traffic
- Discard legitimate traffic

New DDoS Attack

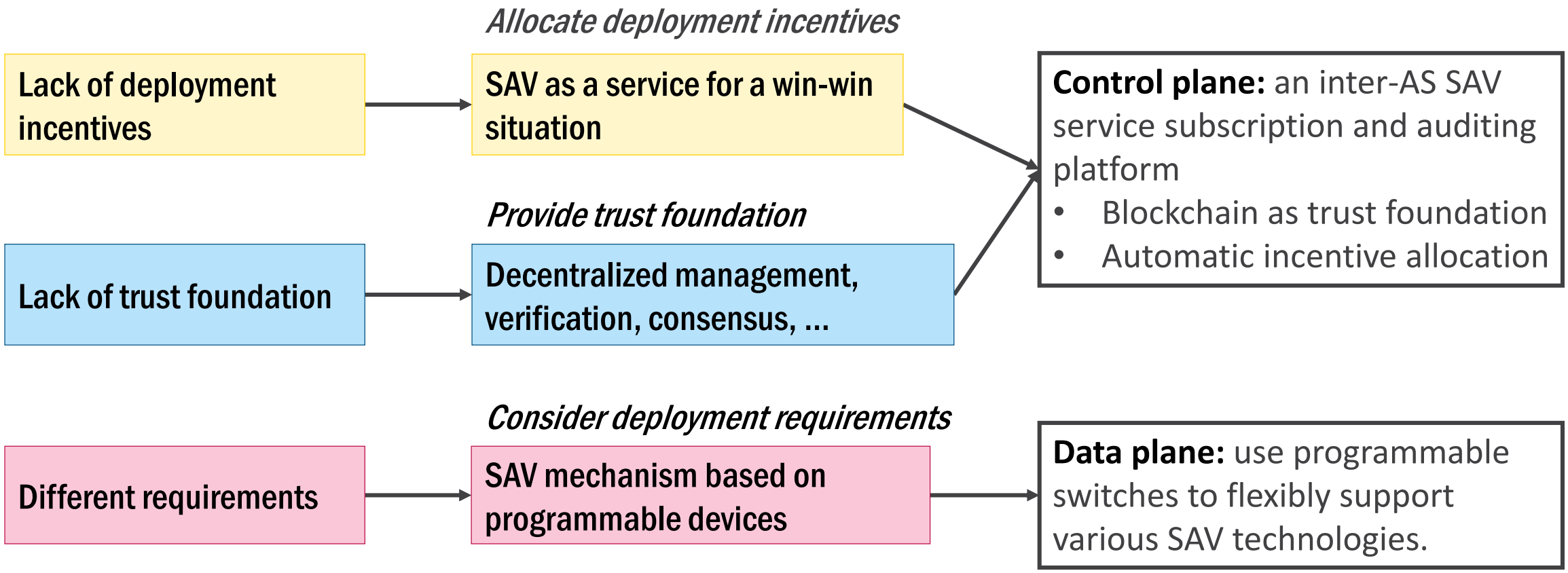
Inter-AS SAV faces deployment challenges



Different deployers have different requirements:

- Labeling-based SAV
- Routing-based SAV

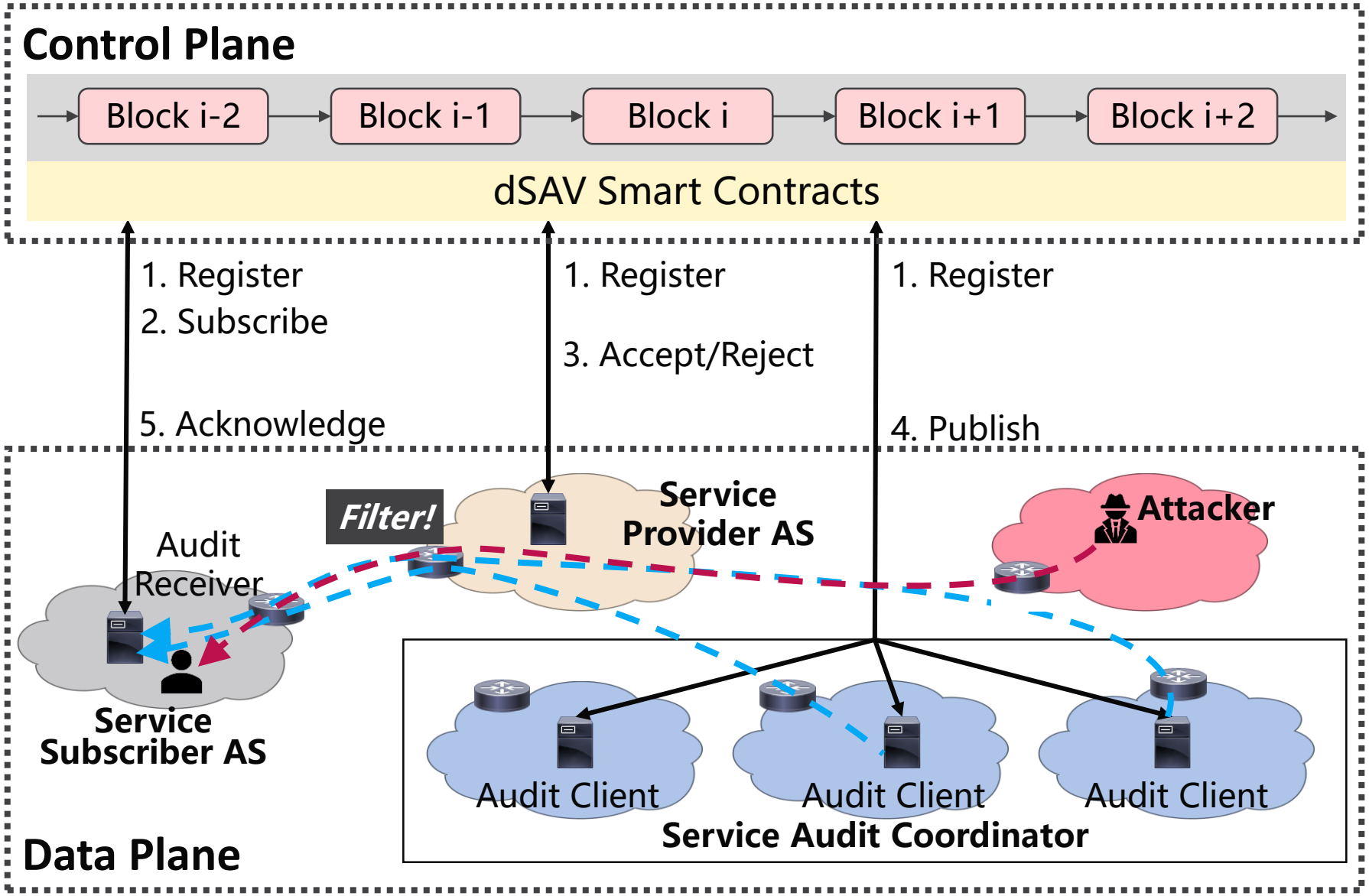
pSAV: A Practical and Decentralized Inter-AS Source Address Validation Service Framework



Talk Outline

- Motivation
- **pSAV Architecture**
  - Control Plane
  - Data Plane
- Some Evaluation Results
- Conclusion

pSAV Architecture



- Control plane: blockchain-based service subscription and auditing platform
- Data plane: SAV implementation on programmable switches

Talk Outline

- ~~Motivation~~
- pSAV Architecture
  - **Control Plane:** blockchain-based service subscription and audit platform
  - **Data Plane:** SAV implementation on programmable switches
- Some Evaluation Results
- Conclusion

Control plane: blockchain-based service subscription and audit platform

- **AS Registration**
  - Verify authenticity
- **Service Subscription**
  - Balance auditability and privacy
- **Service Audit**
  - Provide incentives

All ASes must be registered before they join the blockchain.

- **Service subscriber:** packets' characteristics, e.g., IP address
- **Service provider:** SAV services they support
- **Service auditor:** the auditing results

Control plane: blockchain-based service subscription and audit platform

- **AS Registration**
  - Verify authenticity
- **Service Subscription**
  - Balance auditability and privacy
- **Service Audit**
  - Provide incentives

Service transactions on blockchain

- **Plain text**
  - Subscriber, provider, SAV type, …, to allow auditing of the service.
- **Encrypted text**
  - Privacy information about specific filtering rules, to prevent attackers from using this information to steer by the SAV service.

Control plane: blockchain-based service subscription and audit platform

- **AS Registration**
  - Verify authenticity
- **Service Subscription**
  - Balance auditability and privacy
- **Service Audit**
  - Provide incentives

Subscribers can know whether spoofed packets from auditors are filtered. (*See more in our paper!)*

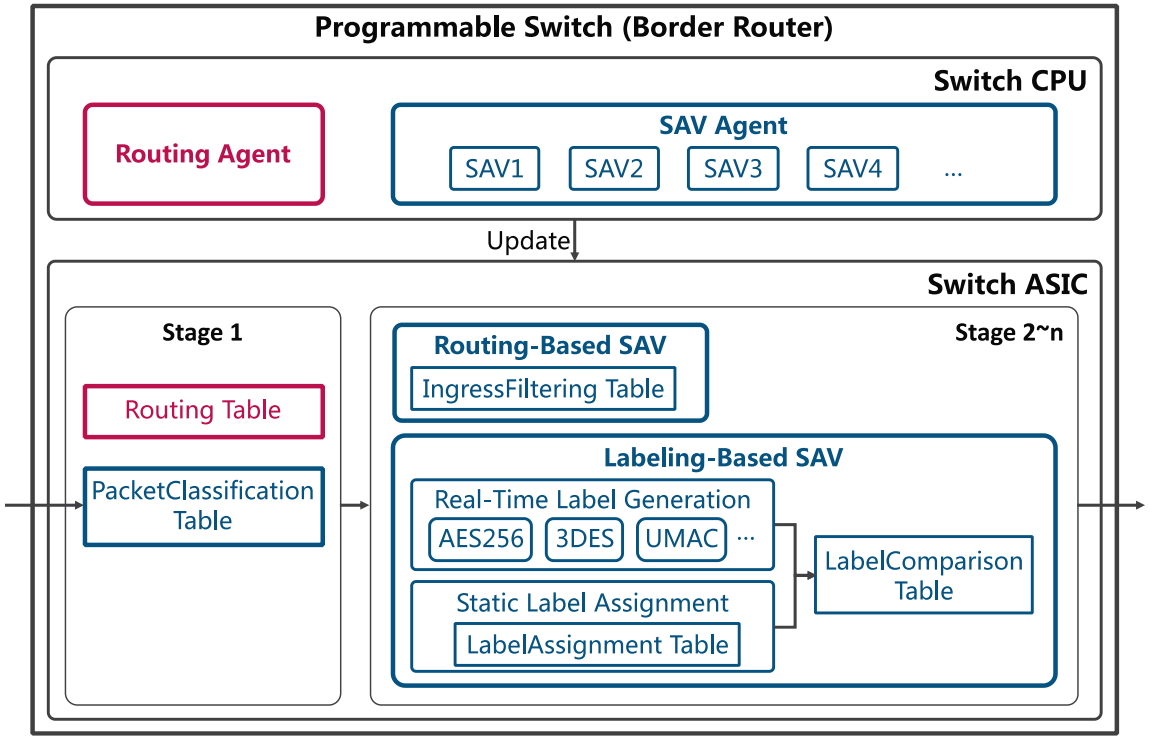
Once audit results are confirmed by subscribers, *incentives are automatically redistributed to auditors from providers.*

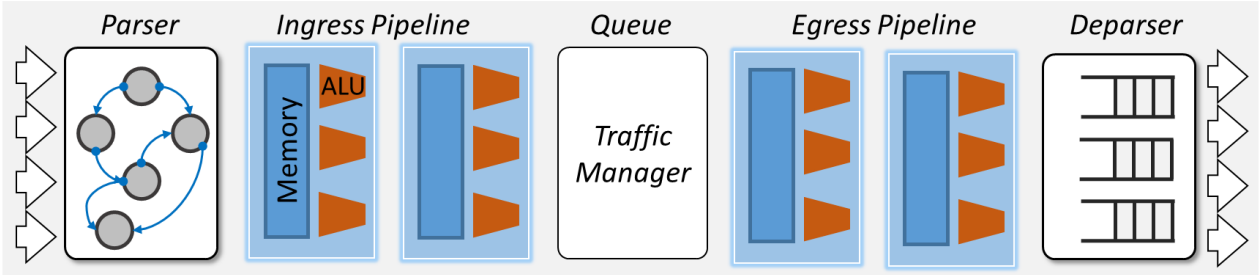
Data plane: SAV implementation on programmable switches

- **Help service providers to accommodate various SAV technologies flexibly.**
  - Routing-based SAV
  - Labeling-based SAV

- Challenge: support various label generation algorithm (e.g., DES, AES) on programmable switches
- Solution: optimization with exact match
- *Some more in our paper!*

See more in our paper!





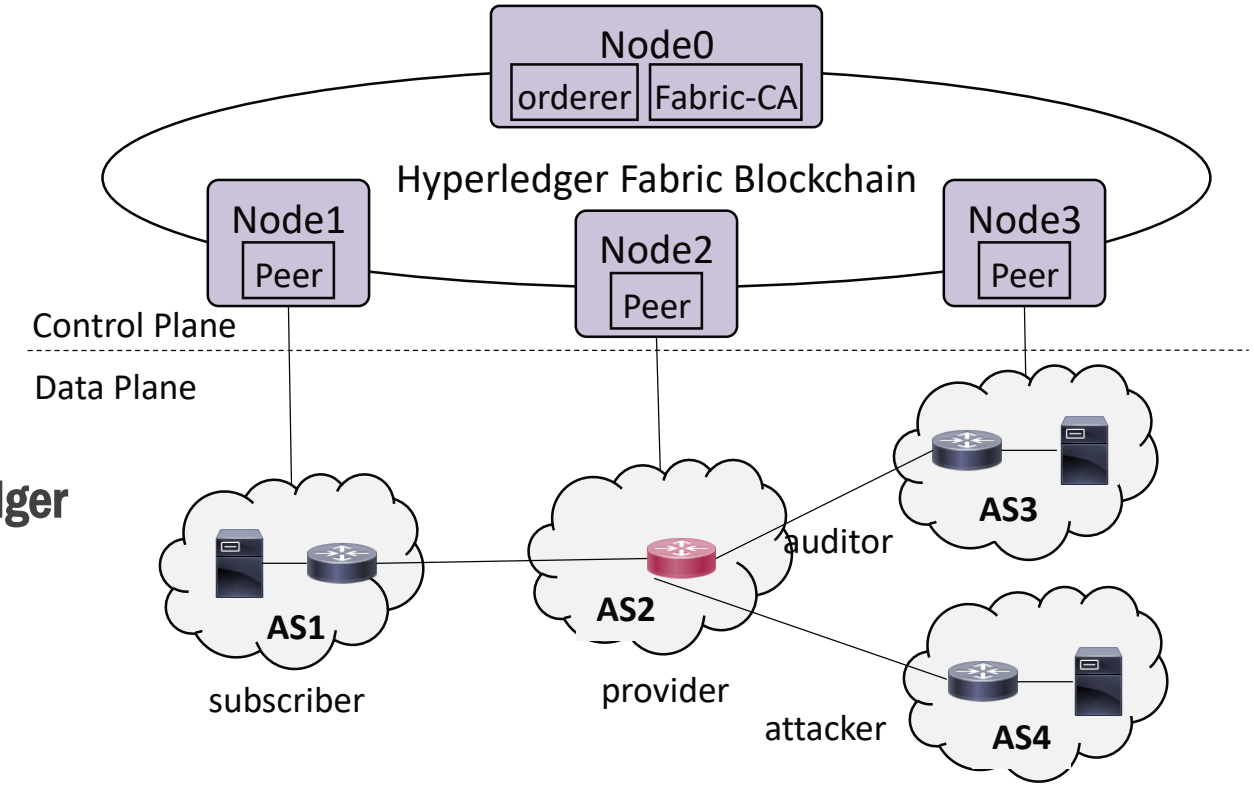
[RMT@SIGCOMM'13]

Talk Outline

- ~~Motivation~~
- pSAV Architecture
- Control Plane
- Data plane
- **Some Evaluation Results**
- Conclusion

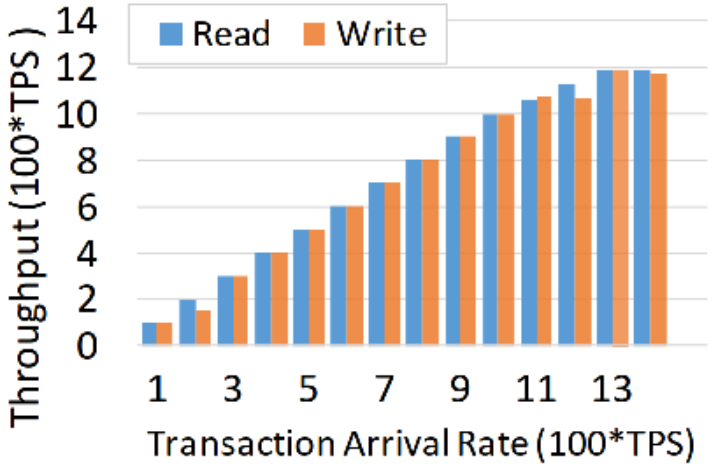
Evaluation Setup

- **Data Plane: a network composed of four ASes with two Intel Tofino switches and three servers**
  - Subscriber AS1
  - Provider AS2 (Intel Tofino switch)
  - Auditor AS3
  - Attacker AS4
- **Control Plane: a test blockchain built with HyperLedger Fabric with one server**
  - SAV contracts with 650 lines of GO language

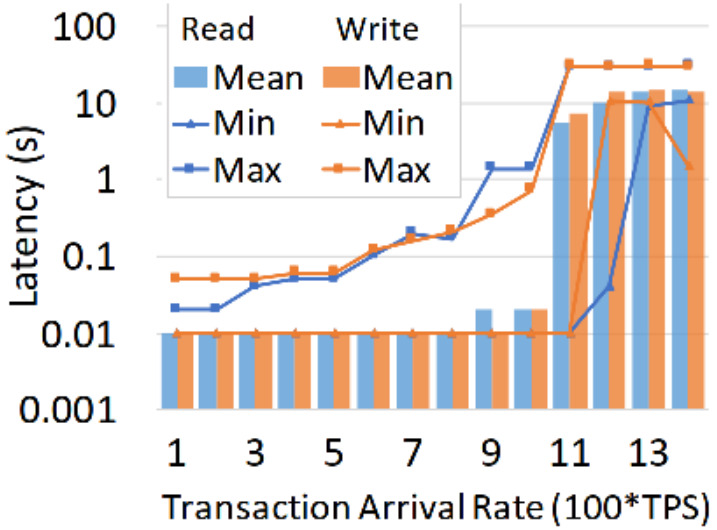


Blockchain performance on control plane

- **Transaction throughput and latency on the control plane.**
  - Write-related transactions: registration, service request from the subscriber, response from the provider, audit result submission from the auditor, and confirmation from the subscriber.



(a) Transaction throughput.



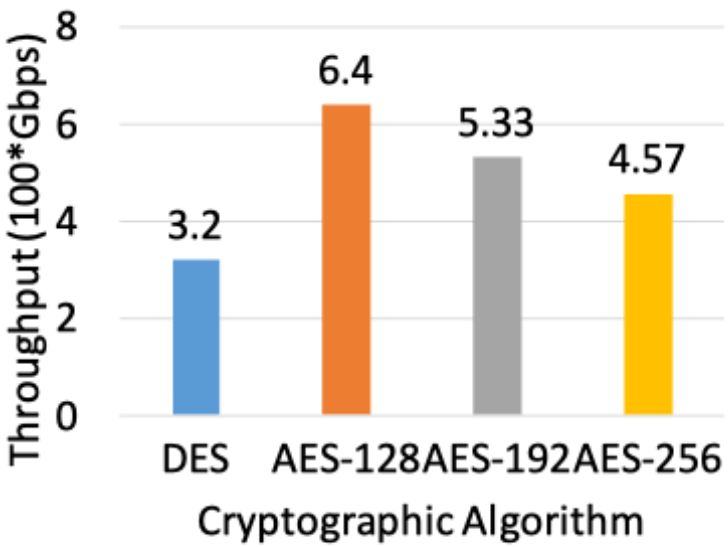
(b) Transaction latency.

Support > 1000 transactions per second.

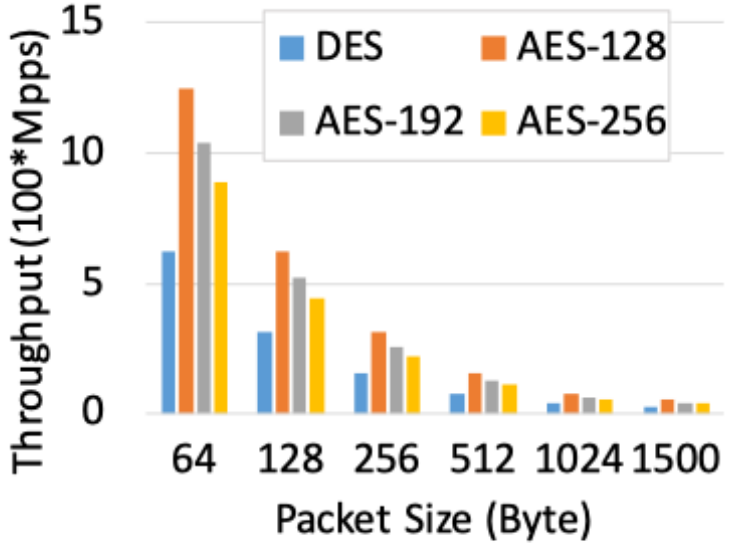
Latency < 1s when there are < 900 transactions per second.

SAV Performance on Data Plane

- **Throughput: labeling-based SAV with various label generation methods on the Tofino switch.**



(a) Gbps under all packet sizes.



(b) Mpps under different packet sizes.

- All have > 100 Gbps throughput in line rate
- Larger throughput means larger service capacity and more revenues

Talk Outline

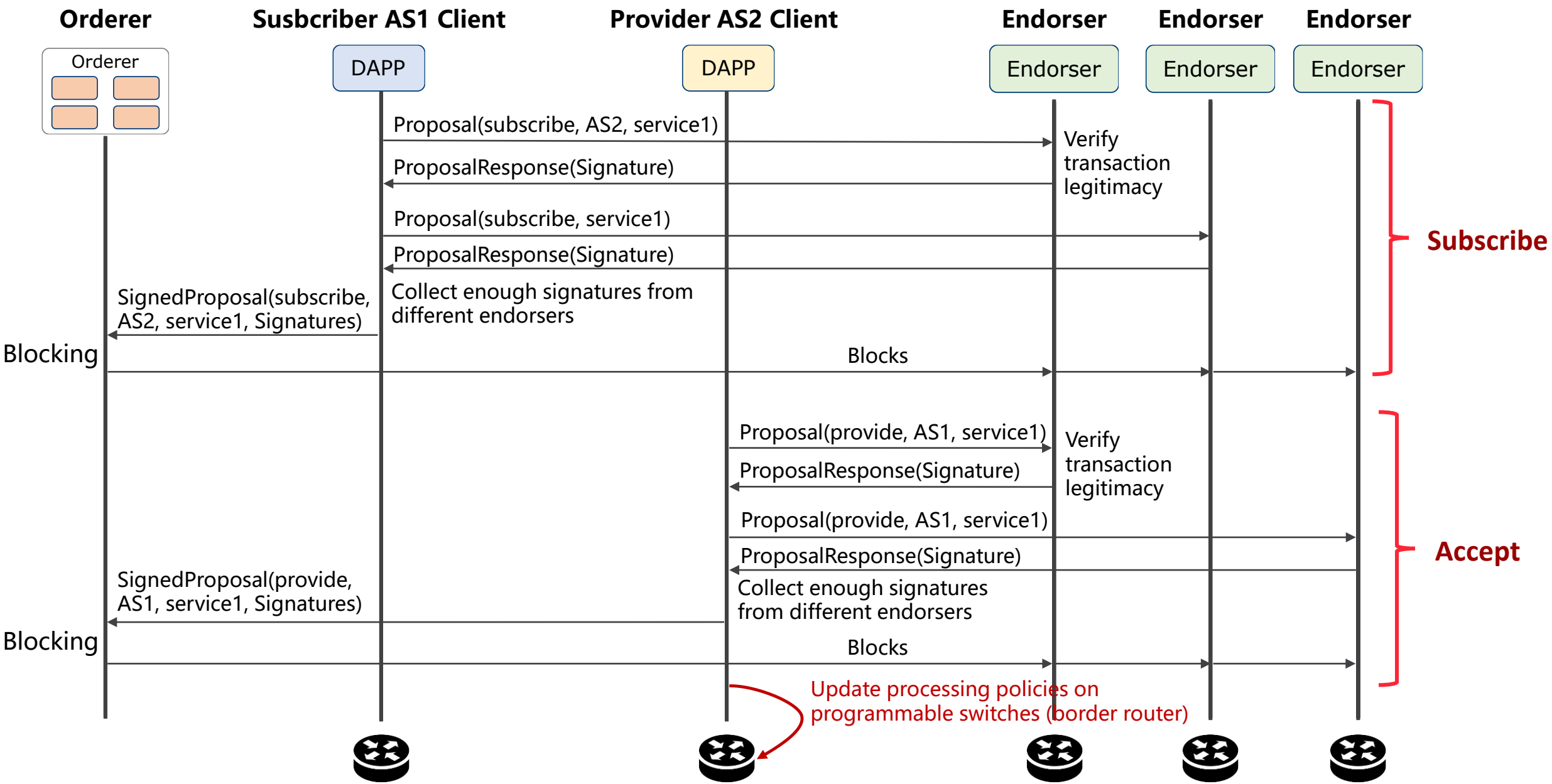
- ~~Motivation~~
- pSAV Architecture
- Control Plane
- Data plane
- Some Evaluation Results
- **Conclusion**

Conclusion

- **pSAV is a practical and decentralized inter-AS source address validation (SAV) service framework to promote inter-AS SAV deployment.**
  - Take SAV as a payable service by dividing participant ASes into service subscribers, providers, and auditors.
  - On the control plane, leverage blockchain as the trust foundation to
    - enable service providers accountable for their offered services
    - allocate incentives to auditors for detecting unqualified services.
  - On the data plane, propose a flexible, high-performance, and low-cost SAV implementation mechanism for providers.

Thanks!

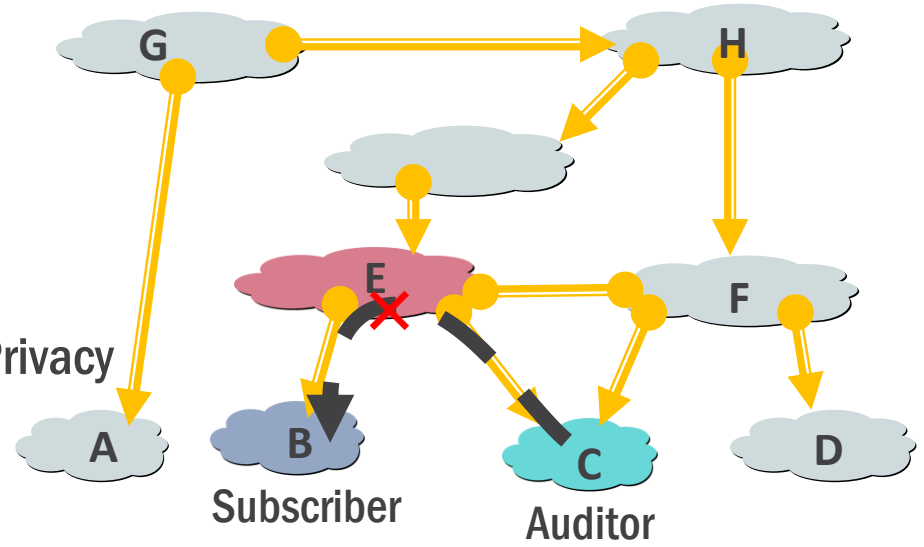
Service subscription and response are all blockchain transaction

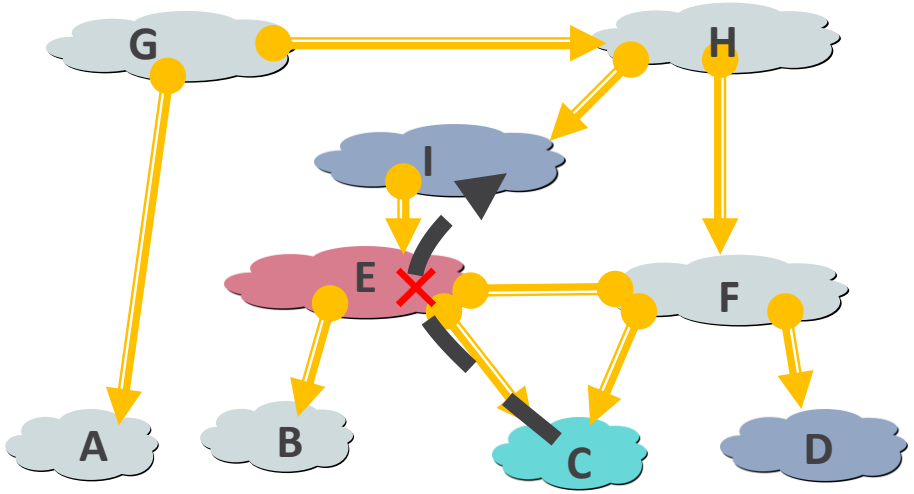


Control plane: blockchain-based service subscription and audit platform

- **AS Registration**
  - Verify Authenticity
- **Service Subscription**
  - Balance Auditability and Privacy
- **Service Audit**
  - Provide Incentives

Subscriber confirm -> incentives are automatically redistributed to auditor from provider.





Flooding-type

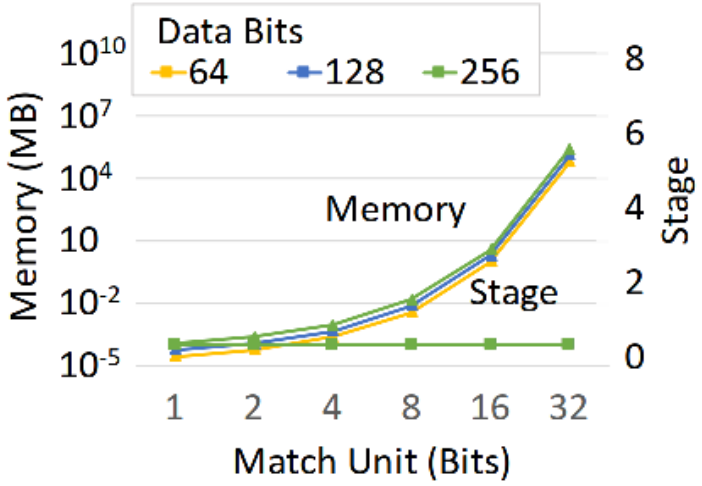
- **Subscriber B**: packets **sent to B** should carry some label
- Auditor C: send spoofed packets to B with IP addresses of A

Reflection-type

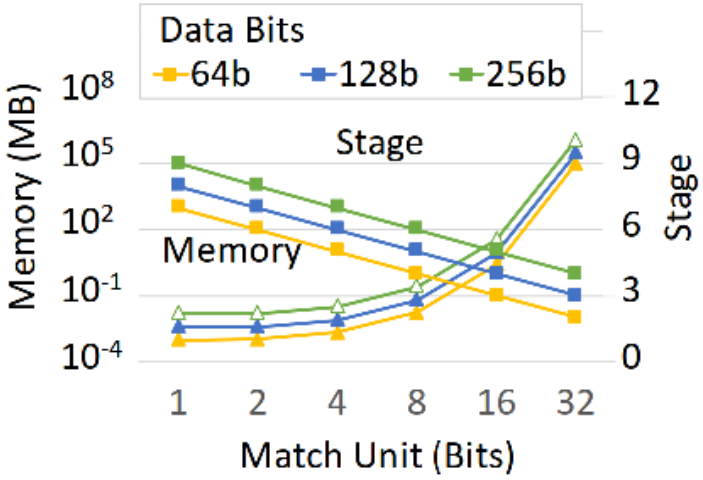
- Subscriber B: packets from B should carry some label
- Auditor C: send spoofed packets to other Ases (e.g., A) with IP addresses of B

SAV Overhead on Data Plane

- **Memory and Stage Overhead of various blocks in Cryptographic computation**
  - Permutation and mixcolumn: with the match unit width increasing, they require more SRAM and fewer stages.
  - Substitution: the stage number is always one.
  - When we take an 8-bit match unit, even 128-bit permutation and mixcolumn operation require five stages and [illegible] M in programm[illegible]



(a) Substitution.



(b) Permutation and MixColumn.