SMG: A Signed Group of Multiple-Origin ASes for Use in the Resource Public Key Infrastructure (RPKI)

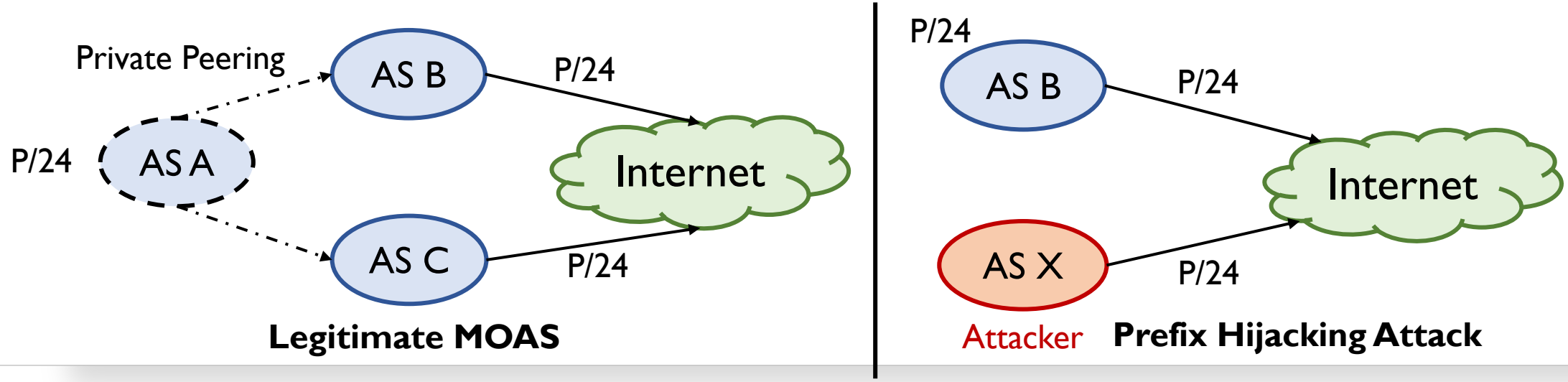
Qi LI
Zhongguancun Laboratory

On behalf of other coauthors: Ke XU, Zhuotao LIU, Qi LI, Jianping WU

https://datatracker.ietf.org/doc/draft-li-sidrops-rpki-moasgroup/

Introduction

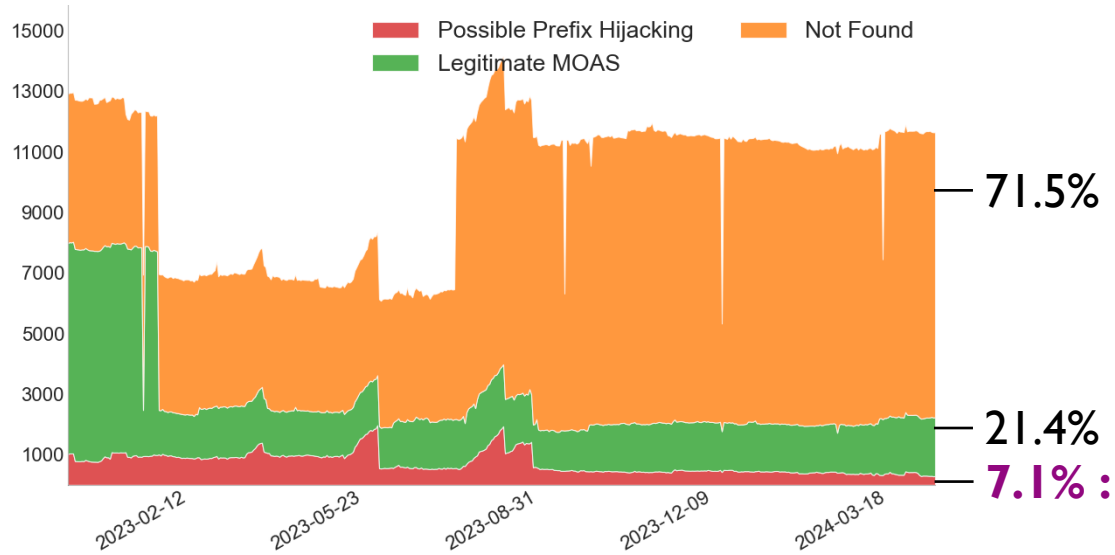
- RFC1930: One prefix, one origin AS
- The prevalence of legitimate Multiple Origin ASes (MOAS) in Internet routing
  - DoS/DDoS mitigation services
  - Business considerations for network traffic optimization
  - Internet eXchange Points (IXPs) for efficient interconnection
- Distinguishing between prefix hijacking, misconfiguration, and legitimate MOAS can be complex.



For detailed analysis see our problem statement draft: https://datatracker.ietf.org/doc/draft-jiang-sidrops-psvro/

Measurement

- Limitations in routing origin registries leave legitimate MOAS vulnerable
- Existing ROV systems may not adequately distinguish legitimate MOAS from malicious attacks, potentially misclassifying legitimate traffic

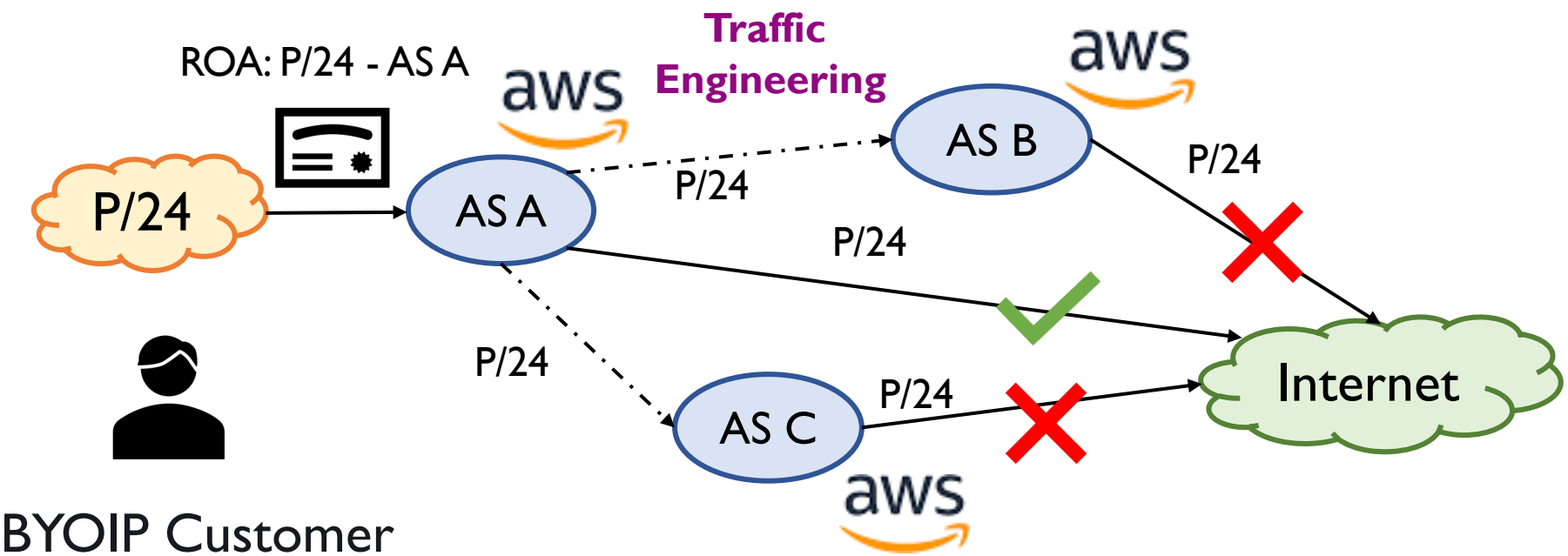


	# of Possible Hijacking Events Per Day
Cisco BGPStream	~8
BGPWatch	~34
Cloudflare Radar	~64

BGPStream: bgpstream.com
BGPWatch: bgpwatch.cgtf.net
Cloudflare Radar: radar.cloudflare.com/routing
CAIDA Dataset: publicdata.caida.org/datasets/routing

Problem Analysis

- ROAs indicate an authority by the prefix holder for some nominated ASes to originate a BGP route for the prefix
- The authorized AS needs to collaborate with other ASes to achieve business goals
- Managing ROAs in collaborative routing is complex
  - Temporary announcement, authorization granularity, operation overhead



Same Organization:

Prefix: 207.45.160.0/20	
AS17378	Valid
AS11383	Invalid
AS17113	Invalid

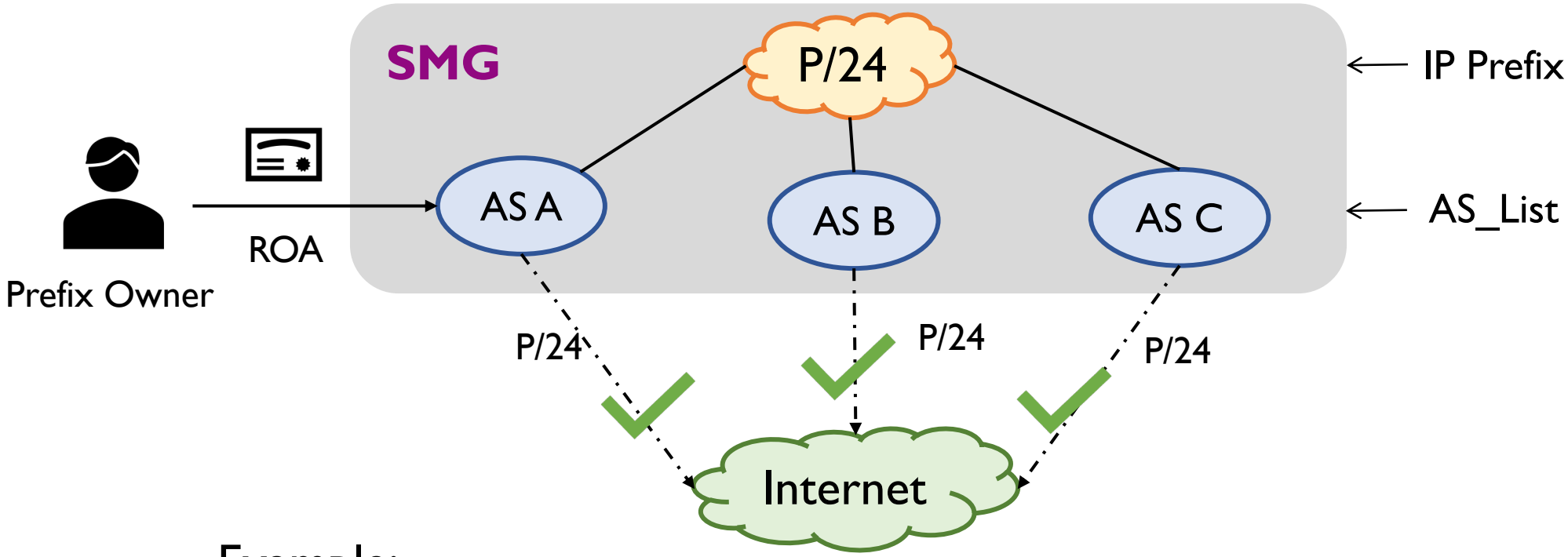
Provider-Customer:

Prefix: 2804:cf4::/32	
AS52579	Valid
AS203	Invalid

*BYOIP: Bring your own IP addresses

Our Proposal: Signed MOAS Group (SMG)

- Signed MOAS Group (SMG): Asserts that a group of ASes intended to collaboratively announce an IP prefix



Example:

Signed MOAS Group Object: P/24 {AS A, AS B, AS C}

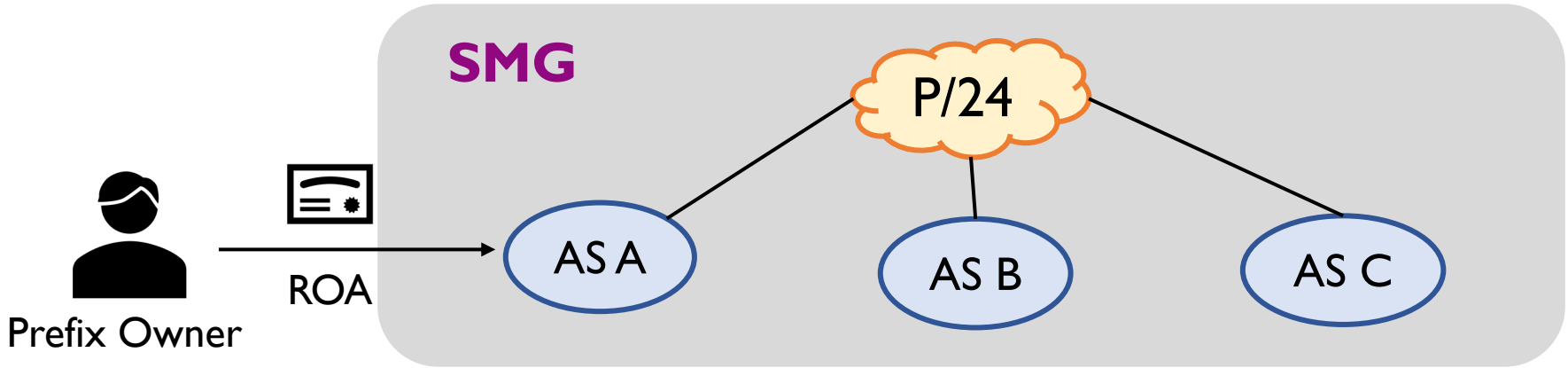
An Example of SMG object

- SMG objects follow the Signed Object Template for the RPKI in RFC6488
- Below is an example of a DER-encoded Signed MOAS Group eContent Payload provided with annotation following the '#' character
- Example: {0, [65536, 65537, 65538], 0001, 192.0.2.0/24}

```
$ echo
3029020100a00f020301000002030100010203010002130430303031030d003139322e302e322e
302f3234 | xxd -r -ps | openssl asn1parse -inform DER -i -dump
    0:d=0  hl=2 l=  41 cons: SEQUENCE
    2:d=1  hl=2 l=   1 prim:  INTEGER           :00     # Version 0
    5:d=1  hl=2 l=  15 cons:  cont [ 0 ]
    7:d=2  hl=2 l=   3 prim:   INTEGER          :010000 # AS65536
   12:d=2  hl=2 l=   3 prim:   INTEGER          :010001 # AS65537
   17:d=2  hl=2 l=   3 prim:   INTEGER          :010002 # AS65538
   22:d=1  hl=2 l=   4 prim:  PRINTABLESTRING   :0001   # IPv4
   28:d=1  hl=2 l=  13 prim:  BIT STRING
      0000 - 00 31 39 32 2e 30 2e 32-2e 30 2f 32 34      # 192.0.2.0/24
```

Issue an SMG based on Aggregate Signature

0. The prefix owner authorized prefix (P/24) to an AS (named authorized AS, noted as AS A in this example) by ROA. [Highly RECOMMEND]
1. The authorized AS (A) initiates a Signed MOAS Group (SMG) object
   - P/24 {AS A, AS B, AS C}
2. The authorized AS (A) sends the SMG object to other ASes (B/C) listed on the object
3. Each listed AS (A/B/C) signs the hash of the SMG object by its private key and sends its individual signature to the authorized AS (A).
4. The authorized AS (A) verifies all the individual signatures and aggregates them into a single "global signature" which will be attached to the SMG object.



SMG Validation

0. The relying party (RP) performs all the validation checks outlined in RFC6488
1. Signature Verification
   - RP aggregates the public keys of all ASes in the AS_List into a single "global key"
   - RP uses the global key to verify the global signature attached to the SMG
2. Consistency Check
   - RP checks the existence of a corresponding ROA for the IP prefix advertised in the SMG, ensuring the advertised prefix in the ROA matches that within the SMG, and the ASN within the ROA must be present in the AS_List of the SMG.

State-Space of SMG Validation

	Signature Verification	Consistency Check	State
1	True	True	Valid
2	True	False	Suspicious
3	False	-	Invalid

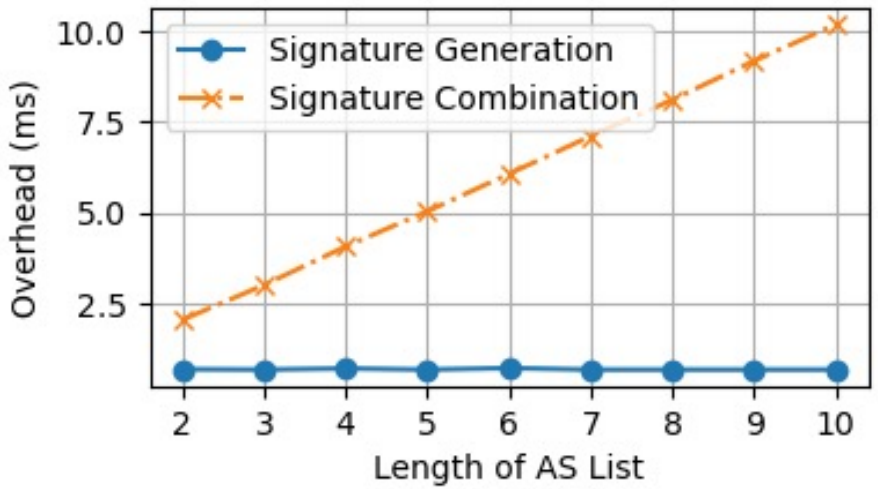
Interaction Between ROA-ROV and SMG-ROV

- SMG makes no change to ROA verification. It is designed to augment and integrate with the existing ROA-ROV procedures. The procedure of SMG-ROV is independent of the current ROA-ROV.
- The specific configuration of a mitigation policy is at the discretion of the network operator. However, the following mitigation policy is highly recommended.

	ROA-ROV	SMG-ROV	Route Selection
1	Valid	-	Accept
2	Invalid	Valid	Accept
3		Suspicious	Recommend Accept
4		Invalid & NotFound	Reject
5	Not Found	Valid	Accept
6		Suspicious	Recommend Accept
7		Invalid & NotFound	Reject

Performance Evaluation

- We implemented a prototype version of SMG in GoLang and integrated it into OctoRPKI
- We evaluated the performance of the SMG protocol on MacOS with an 8-core CPU and 16GB memory.
- Issuing an SMG including 3 ASes only takes about 4.13ms (0.44+0.68+3.01) overhead and RP only needs 1.01ms overhead to validate it.



Operation	Overhead (ms)
SMG Object Initiation	0.44
SMG Validation	1.01

*The overhead of checking the consistency of ROAs is not included in SMG validation.

SMG Implementation: https://github.com/liqi16/signed_moas_group

Conclusion

- We proposed a "Signed MOAS Group (SMG)", a Cryptographic Message Syntax (CMS) protected content type to carry an IP prefix and a list of ASes authorized to announce this prefix.
- The SMG allows multiple ASes to announce an IP prefix collaboratively and securely, supporting business partnerships, traffic engineering, and DDoS mitigation scenarios.
- We implemented a prototype version of SMG in GoLang and evaluated the performance of each operation.

See additional details: *https://datatracker.ietf.org/doc/draft-li-sidrops-rpki-moasgroup/*

Thank You!
Questions & Feedback

Comments are welcomed.

Please email feedback to

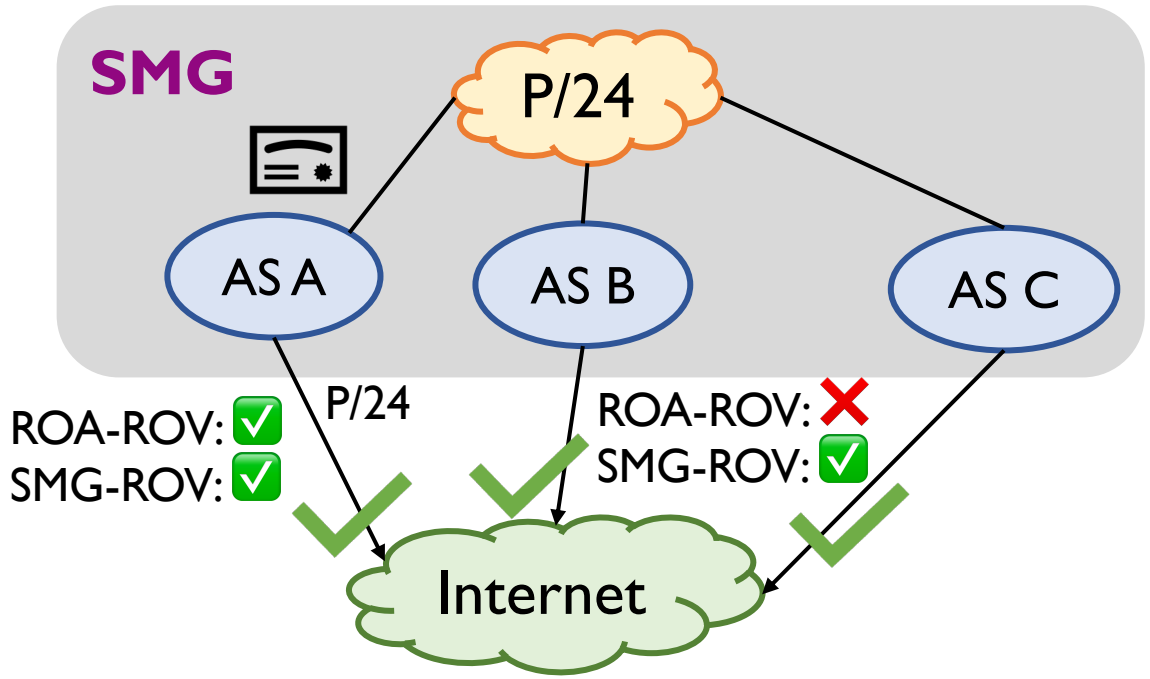
draft-li-sidrops-rpki-moasgroup@ietf.org

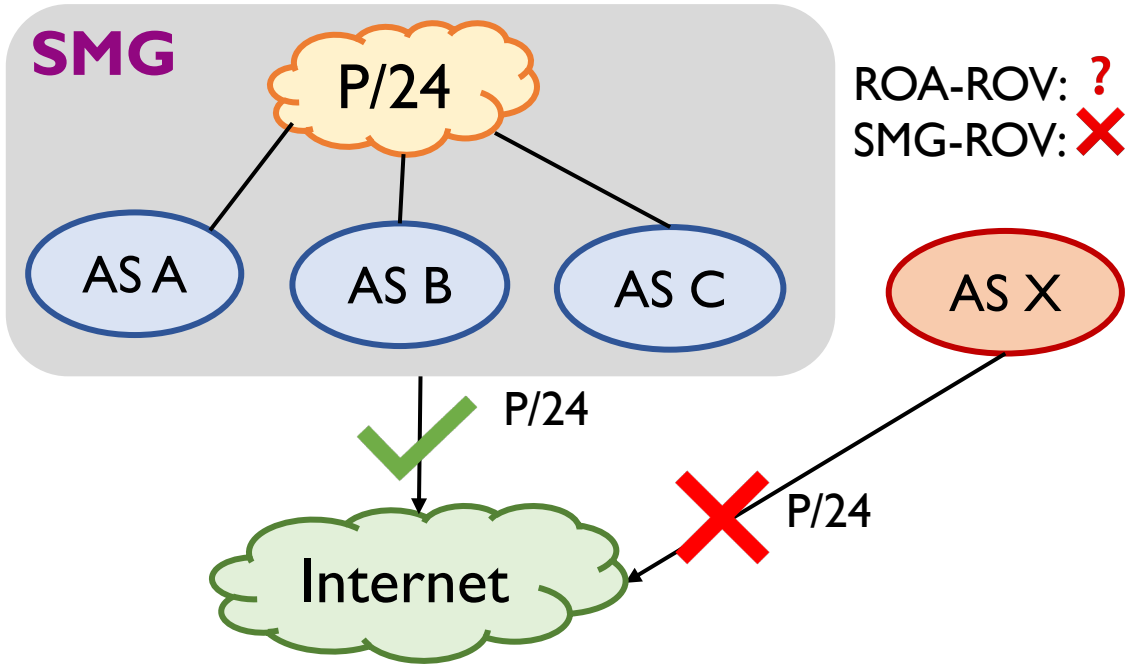
or, open issues at

https://github.com/liqi16/draft-li-sidrops-rpki-moasgroup

Problem Solved by SMG

1. Protecting legitimate MOAS in the network
2. Better distinguish between legitimate and illegitimate MOAS conflicts to defend against prefix hijacking and misconfiguration





*Valid: ✅ Invalid: ❌ NotFound: ?

Operational Consideration

1. BLS Signature: SMG suggests using the BLS signature and BLS12-381 elliptical curve to ensure efficient aggregation.
2. AS Number Sorting: The AS Numbers in the AS_List that are authorized by the ROA should be placed at the beginning of the list, ahead of any non-authorized ASes.
   - RP can only validate the IP prefix and the first ASN by ROAs
   - Improve the efficiency of the RP validation process
3. Multiple valid SMG with the same IP prefix: an AS should only participate in one SMG for the same IP prefix.
   - If the AS_List of an SMG needs modification, it is highly recommended to revoke the current SMG and sign a new one.