FC-BGP:
Towards Secure Inter-domain Routing and Forwarding via Verifiable Routing Commitments

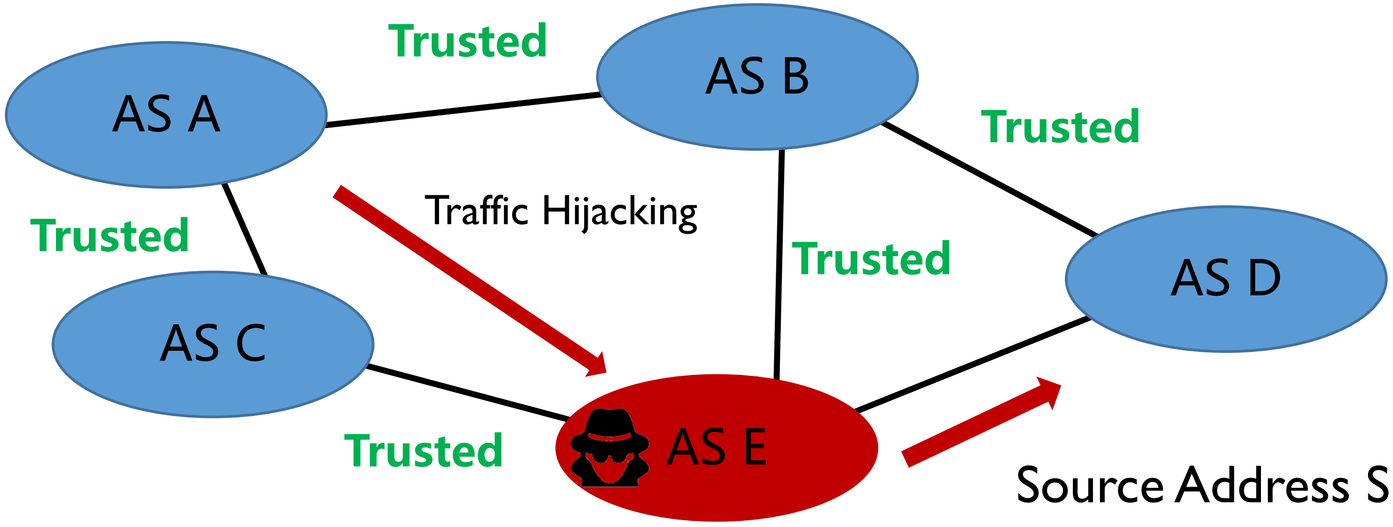
Zhuotao Liu
Tsinghua University

On behalf of coauthors: Ke Xu, Xiaoliang Wang, Qi Li, and Jianping Wu

Background

The current Internet inter-domain routing has vulnerability in both the control plane and the data plane.

- Control plane: no built-in mechanism to verify the BGP announcements
- Data plane: the actual data forwarding path is not consistent with the BGP path



Source Address Spoofing

Forwarding Path Manipulation

Background

BGP Security Enhancements	S-BGP, RPKI and BGPSec, SoBGP, psBGP, Path-end, SBAS
Forwarding Path Validation	ICING, OPT, OSP, PPV, MASK, EPIC
Source Address Validation	SAVA, DPF/IDPF, BCP 38, uRPF, SPM, Passport, IPsec

Threat Model

Assumption: ASes participating in our system (called FC-BGP) have access to an Internet-scale trust base, namely Resource Public Key Infrastructure (RPKI), that stores authoritative information about the mapping between AS numbers and their owned IP prefixes, as well as the public keys of these ASes

Adversary：

(i) On the control plane, the adversary can launch path manipulation attacks. This means that the adversary will try to manipulate routing paths to the victim ASes or sending bogus BGP updates

(ii) On the data plane, the adversary can spoof source addresses and send unwanted network traffic to the victim ASes/prefixes

Goals

Security

Enhance the security of inter-domain routing and forwarding:

- Authenticating the BGP announcements on the fly
- Ensuring that the data plan forwarding is consistent with control plane routing decisions

Compatibility and Deployability

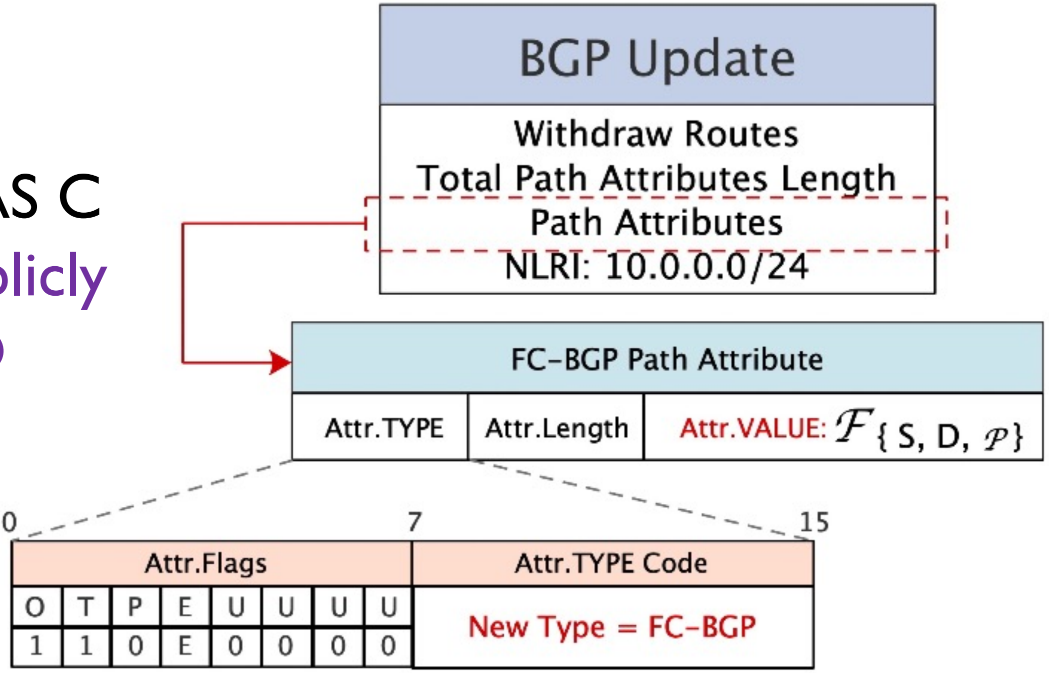
Compatible with the current BGP, and incrementally deployable

Lightweight

No significant performance impact, even in large-scale deployments

Forwarding Commitment

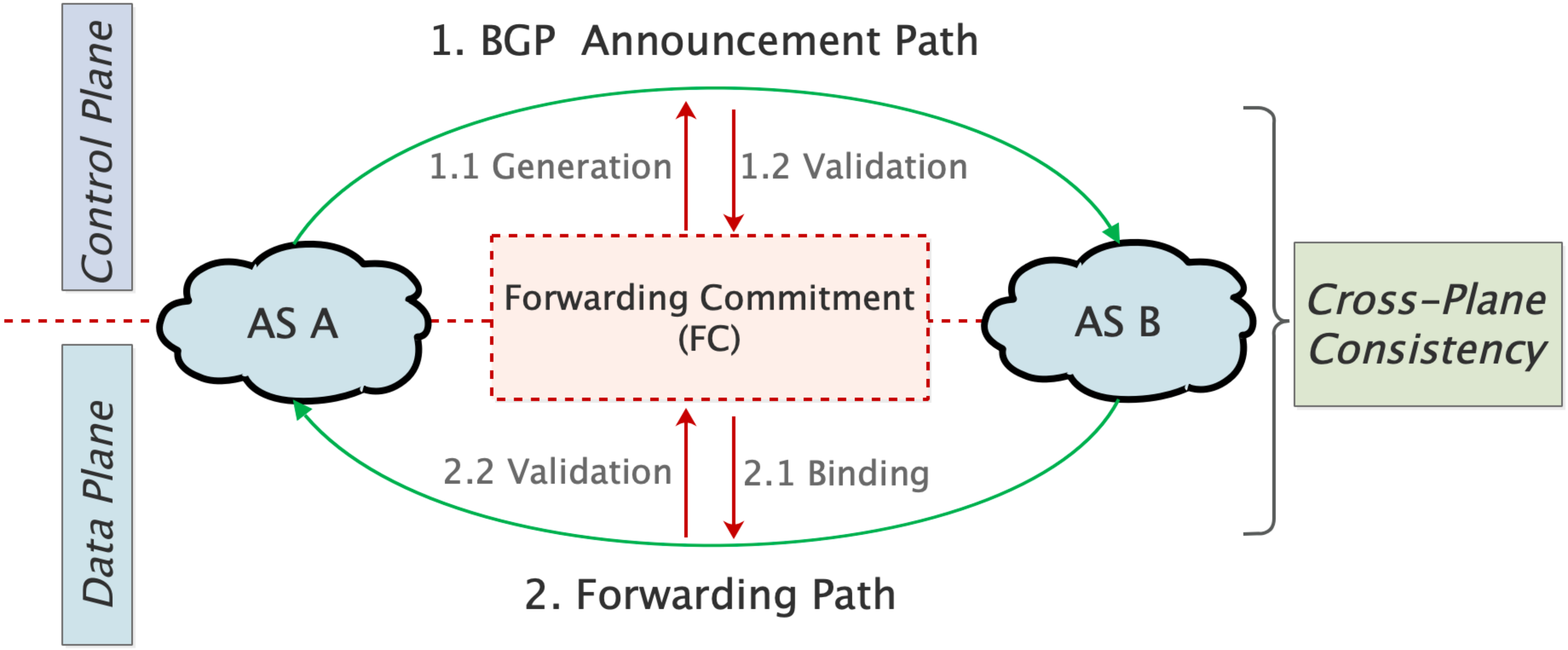
Suppose AS C receives a BGP update P:$S \leftarrow A \leftarrow C$, AS C uses the following Forwarding Commitment to publicly certify its routing intent over the next hop to AS D



$$\mathcal{F}_{\{C,D,\mathcal{P}\}} = \left\{\mathcal{H}(C,D,\mathcal{P})_{\text{Sig}_C} \;||\; \text{C} \;||\; \text{D}\right\}$$

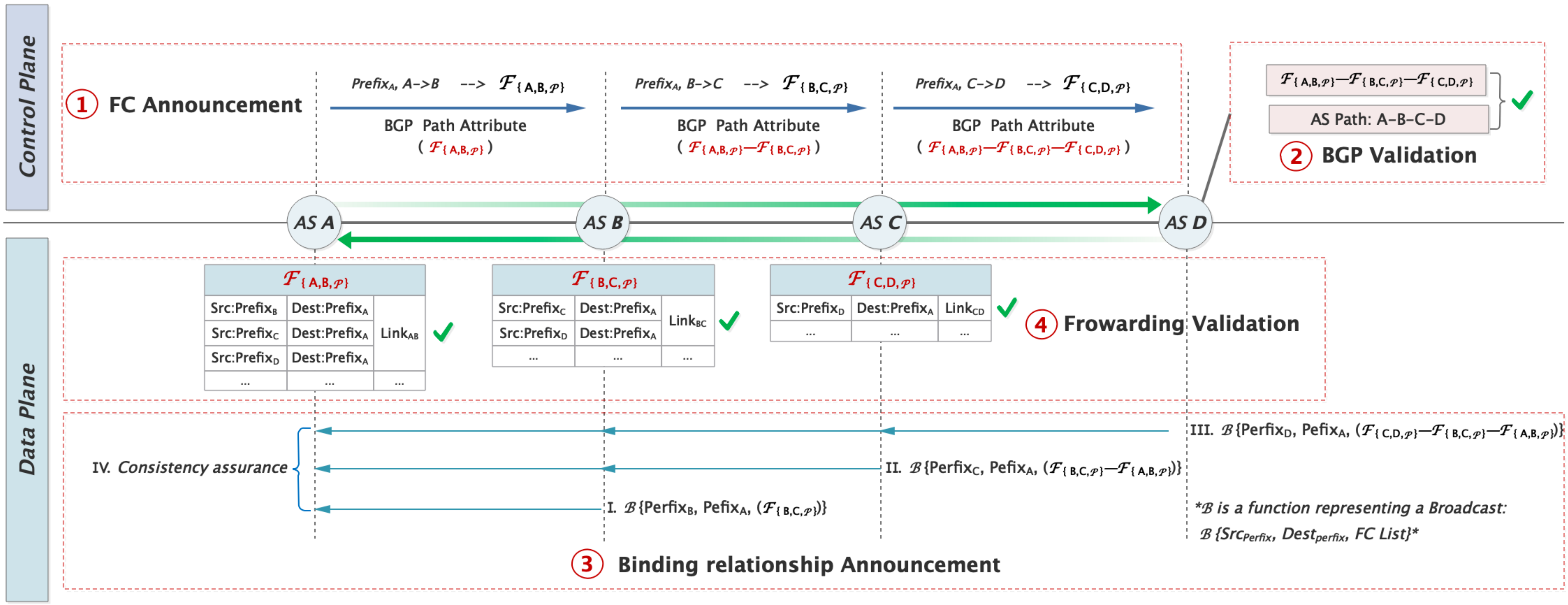
(i) Ensuring that the FCs generated by an AS do not leak its routing preference/policies
(ii) FC-BGP adopts a per-hop verification scheme for validating BGP updates, instead of the per-path verification scheme used in BPGsec

Overview



1. ASes generate FC while processing BGP updates
2. On-path ASes can validate BGP update messages via FCs
3. Backpropagate the FC-list to the on-path Ass (and optionally to off-path ASes)
4. ASes can filter unwanted traffic based on the FC-list

Overview



① FC Announcement

Prefix$_A$, A->B --> $\mathcal{F}_{\{A,B,\mathcal{P}\}}$
BGP Path Attribute
($\mathcal{F}_{\{A,B,\mathcal{P}\}}$)

Prefix$_A$, B->C --> $\mathcal{F}_{\{B,C,\mathcal{P}\}}$
BGP Path Attribute
($\mathcal{F}_{\{A,B,\mathcal{P}\}}$—$\mathcal{F}_{\{B,C,\mathcal{P}\}}$)

Prefix$_A$, C->D --> $\mathcal{F}_{\{C,D,\mathcal{P}\}}$
BGP Path Attribute
($\mathcal{F}_{\{A,B,\mathcal{P}\}}$—$\mathcal{F}_{\{B,C,\mathcal{P}\}}$—$\mathcal{F}_{\{C,D,\mathcal{P}\}}$)

$\mathcal{F}_{\{A,B,\mathcal{P}\}}$—$\mathcal{F}_{\{B,C,\mathcal{P}\}}$—$\mathcal{F}_{\{C,D,\mathcal{P}\}}$
AS Path: A–B–C–D ✓

② BGP Validation

$\mathcal{F}_{\{A,B,\mathcal{P}\}}$		
Src:Prefix$_B$	Dest:Prefix$_A$	Link$_{AB}$
Src:Prefix$_C$	Dest:Prefix$_A$	
Src:Prefix$_D$	Dest:Prefix$_A$	
...	...	...

✓

$\mathcal{F}_{\{B,C,\mathcal{P}\}}$		
Src:Prefix$_C$	Dest:Prefix$_A$	Link$_{BC}$
Src:Prefix$_D$	Dest:Prefix$_A$	
...	...	...

✓

$\mathcal{F}_{\{C,D,\mathcal{P}\}}$		
Src:Prefix$_D$	Dest:Prefix$_A$	Link$_{CD}$
...	...	...

✓

④ Frowarding Validation

III. $\mathcal{B}$\{Perfix$_D$, Pefix$_A$, ($\mathcal{F}_{\{C,D,\mathcal{P}\}}$—$\mathcal{F}_{\{B,C,\mathcal{P}\}}$—$\mathcal{F}_{\{A,B,\mathcal{P}\}}$)\}

II. $\mathcal{B}$\{Perfix$_C$, Pefix$_A$, ($\mathcal{F}_{\{B,C,\mathcal{P}\}}$—$\mathcal{F}_{\{A,B,\mathcal{P}\}}$)\}

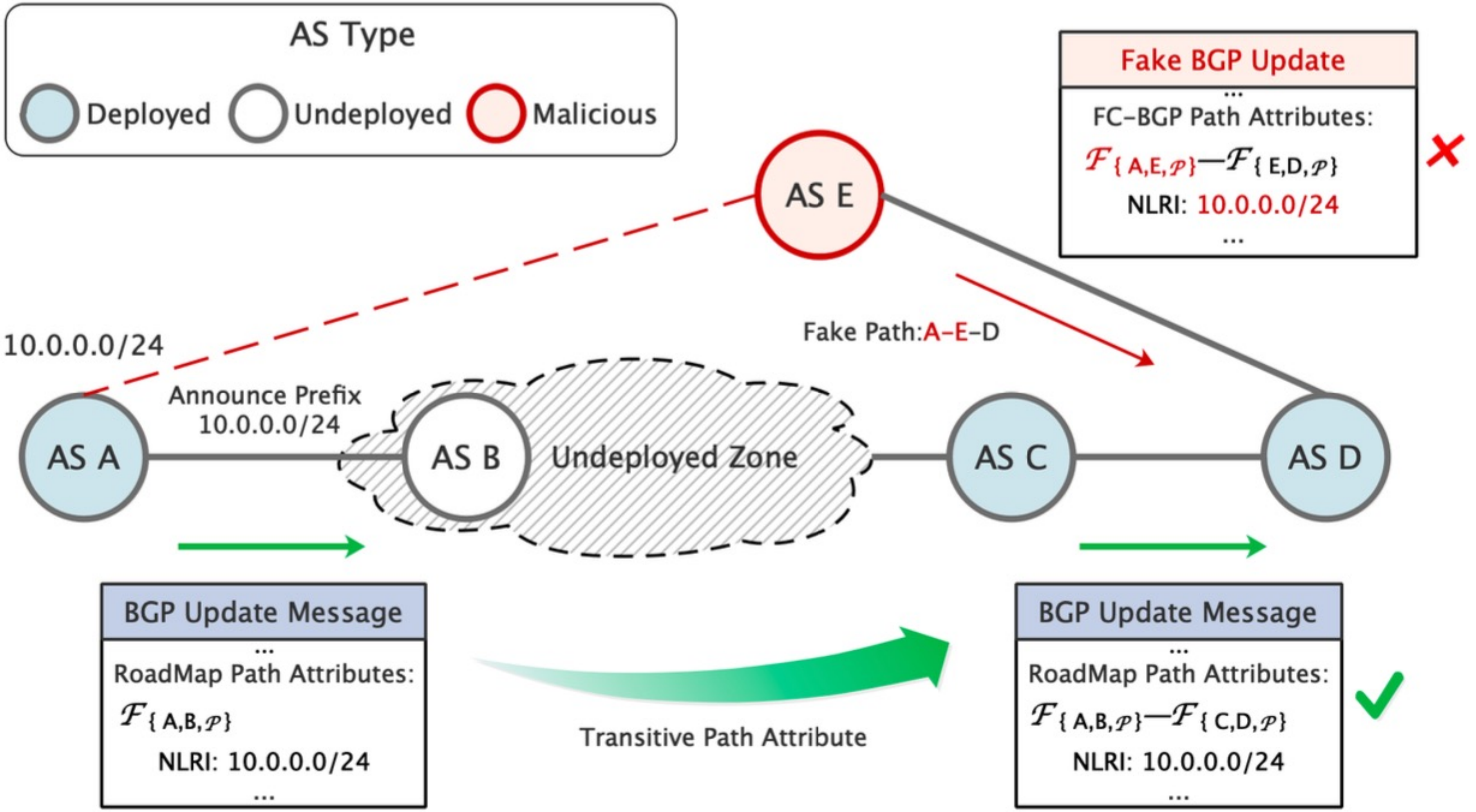
I. $\mathcal{B}$\{Perfix$_B$, Pefix$_A$, ($\mathcal{F}_{\{B,C,\mathcal{P}\}}$)\}

IV. *Consistency assurance*

**$\mathcal{B}$ is a function representing a Broadcast:*
*$\mathcal{B}$ \{Src$_{Perfix}$, Dest$_{perfix}$, FC List\}**

③ Binding relationship Announcement

BGP Path Validation



Fake BGP Update

...

FC–BGP Path Attributes:

$\mathcal{F}_{\{A,E,\mathcal{P}\}}$—$\mathcal{F}_{\{E,D,\mathcal{P}\}}$

NLRI: 10.0.0.0/24

...

✗

BGP Update Message

...

RoadMap Path Attributes:

$\mathcal{F}_{\{A,B,\mathcal{P}\}}$

NLRI: 10.0.0.0/24

...

BGP Update Message

...

RoadMap Path Attributes:

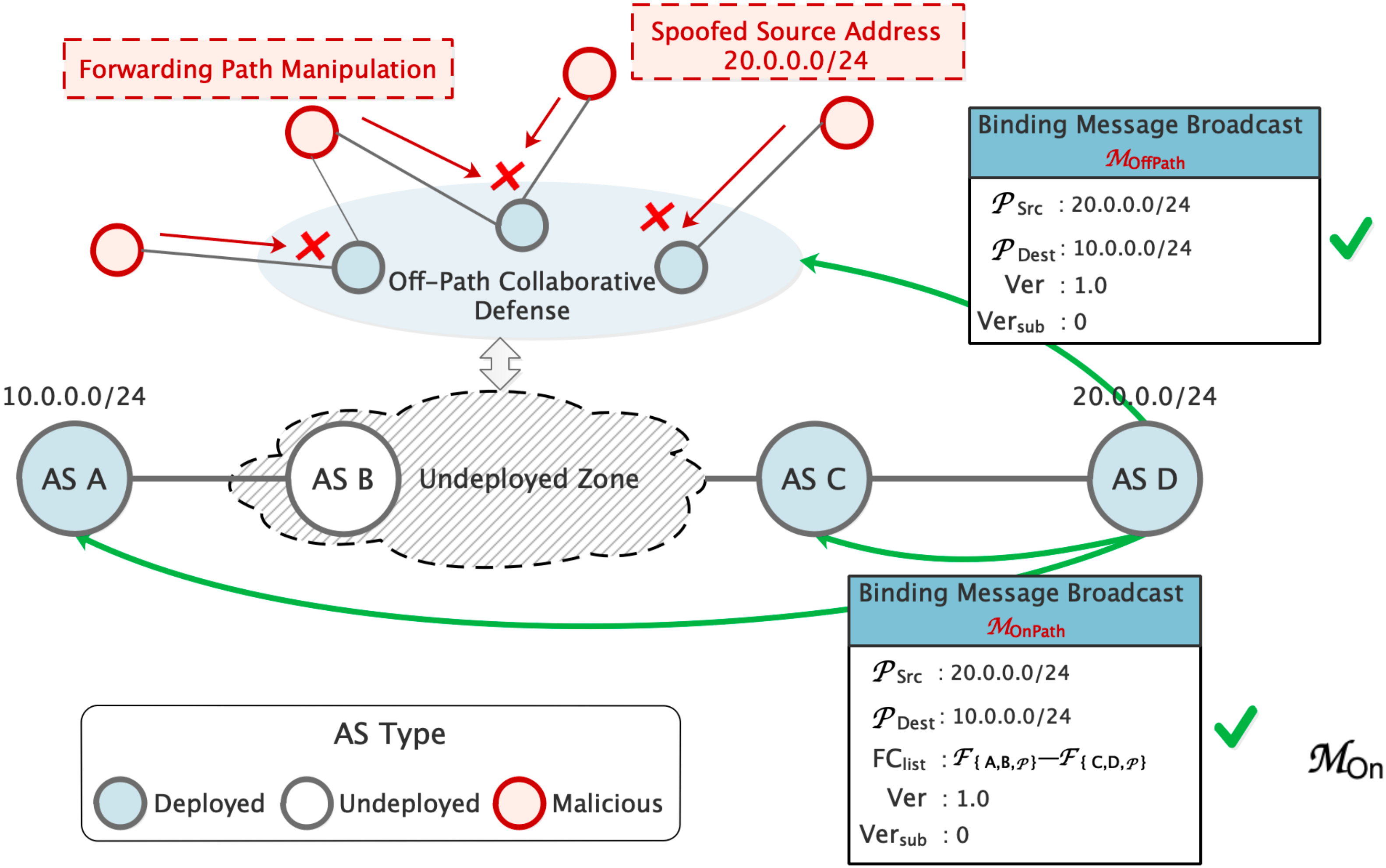
$\mathcal{F}_{\{A,B,\mathcal{P}\}}$—$\mathcal{F}_{\{C,D,\mathcal{P}\}}$

NLRI: 10.0.0.0/24

...

✓

Forwarding Validation



Binding Message Broadcast
$\mathcal{M}_{\text{OffPath}}$

$\mathcal{P}_{\text{Src}}$	: 20.0.0.0/24
$\mathcal{P}_{\text{Dest}}$	: 10.0.0.0/24
Ver	: 1.0
Ver_{sub}	: 0

Binding Message Broadcast
$\mathcal{M}_{\text{OnPath}}$

$\mathcal{P}_{\text{Src}}$	: 20.0.0.0/24
$\mathcal{P}_{\text{Dest}}$	: 10.0.0.0/24
FC_{list}	: $\mathcal{F}_{\{\text{A,B},\mathcal{P}\}}$—$\mathcal{F}_{\{\text{C,D},\mathcal{P}\}}$
Ver	: 1.0
Ver_{sub}	: 0

✓

$$\mathcal{M}_{\text{OffPath}} = \left\{\mathcal{P}_{\text{src}}, \mathcal{P}_{\text{dst}}, \text{Ver}, \text{Ver}_{\text{sub}}\right\}_{\text{Sig}_{\text{src}}}$$

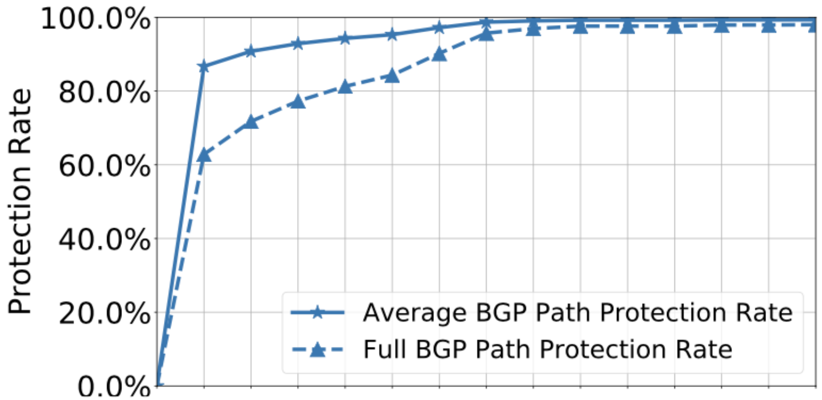
✓

$$\mathcal{M}_{\text{OnPath}} = \left\{\mathcal{P}_{\text{src}}, \mathcal{P}_{\text{dst}}, \text{FC}_{\text{list}}, \text{Ver}, \text{Ver}_{\text{sub}}\right\}_{\text{Sig}_{\text{src}}}$$

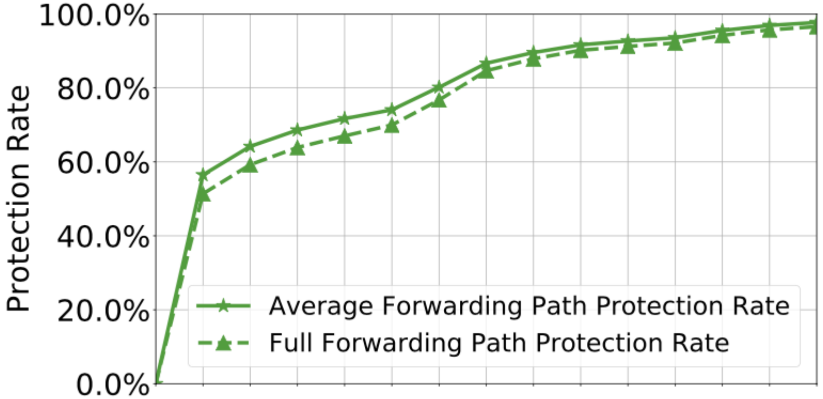
Security Benefits

$$\bar{R} = \frac{R_{\text{BGPpath}}(P)}{K}, \{P|P \in \mathbf{P}\}$$

$$R_{\text{full}} = \frac{|P|}{K} \quad \text{where} \quad \{P \in \mathbf{P} \;\; \text{and} \;\; R_{\text{BGPpath}}(P) = 1\}$$



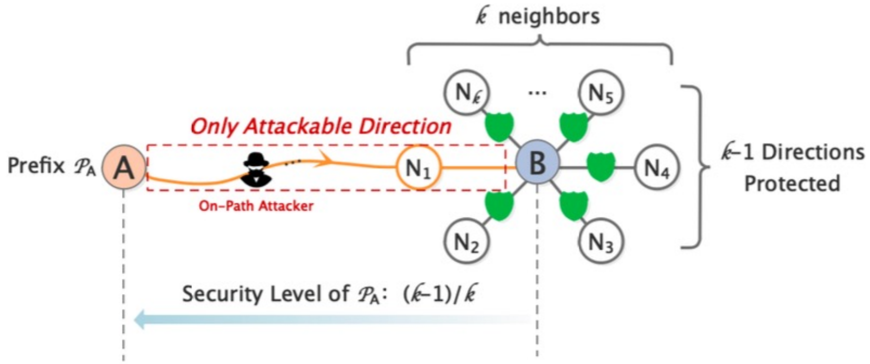
BGP Path Protection

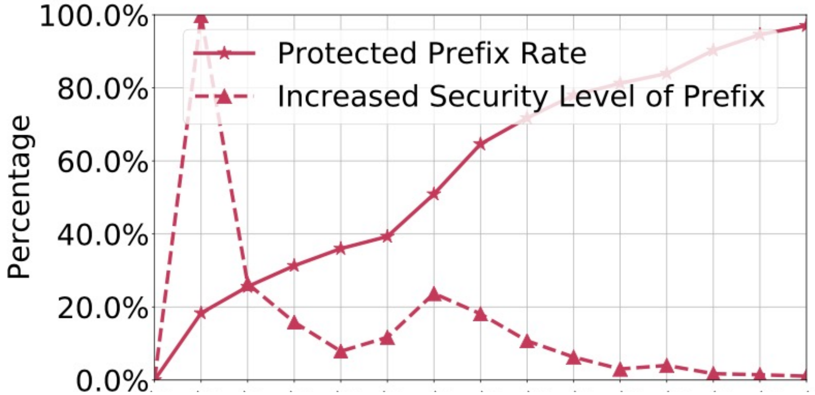


Forwarding Path Protection

$$SLP_{P_A}^{d} = \frac{\sum_{p \in S} \frac{K_p - 1}{K_p}}{|S|}$$

$$\Delta SLP_{d,d_{pre}} = \frac{\sum_{p \in S_d} (SLP_p^{d} - SLP_p^{d_{pre}})}{|S_d|},$$

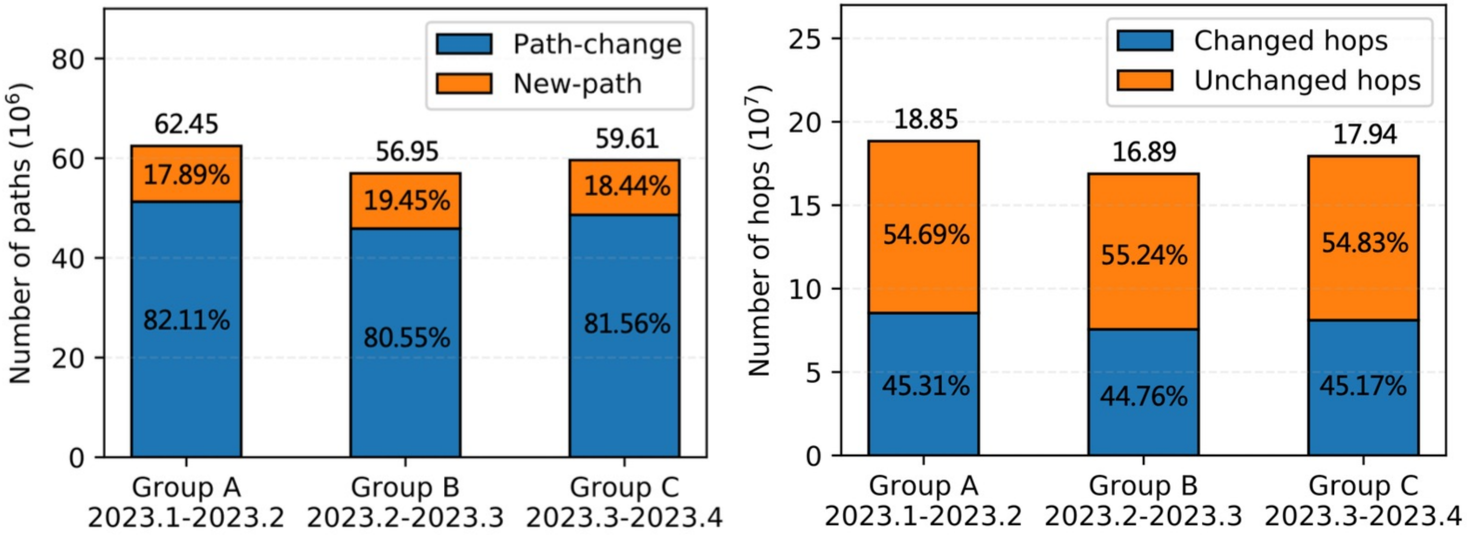




Source Address Protection

Evaluation

1. Internet-Scale BGP Update Validation



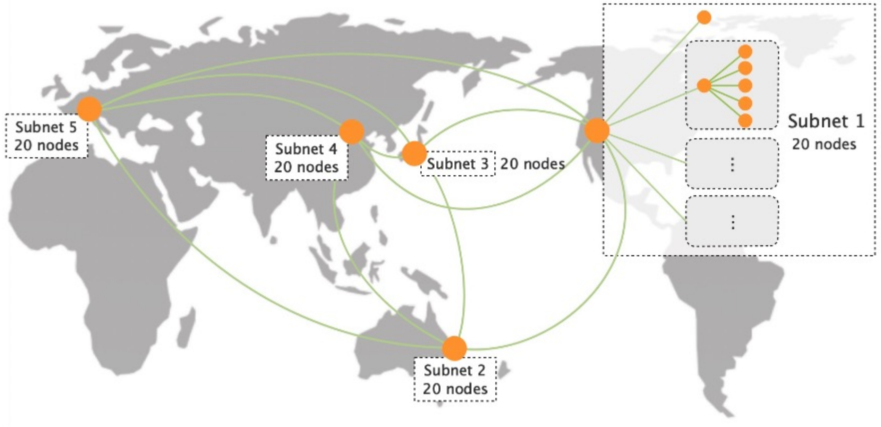
Statistical results of the BGP updates.

- We analyze the BGP announcement dataset collected from January to April 2023
- Over 80% of BGP updates are path-change updates, within which over 55% of hops remain the same
- Over 88% of path-change updates include less than 2 hop changes

Hop-based path verification has much smaller **dynamic verification overhead** than the path-based verification scheme

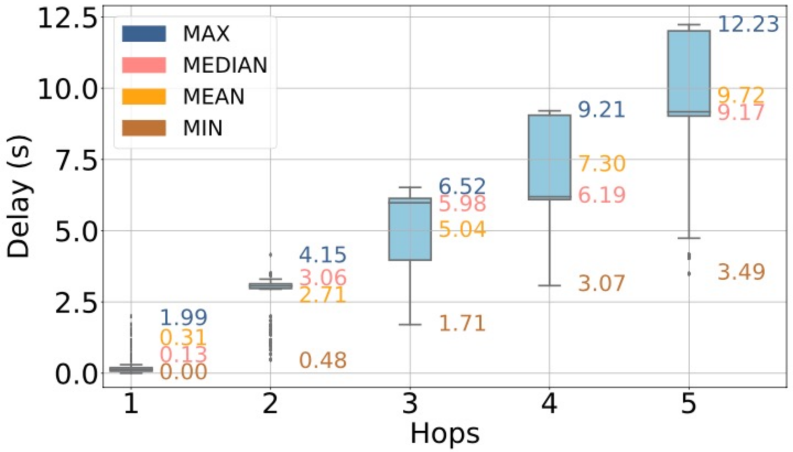
Evaluation

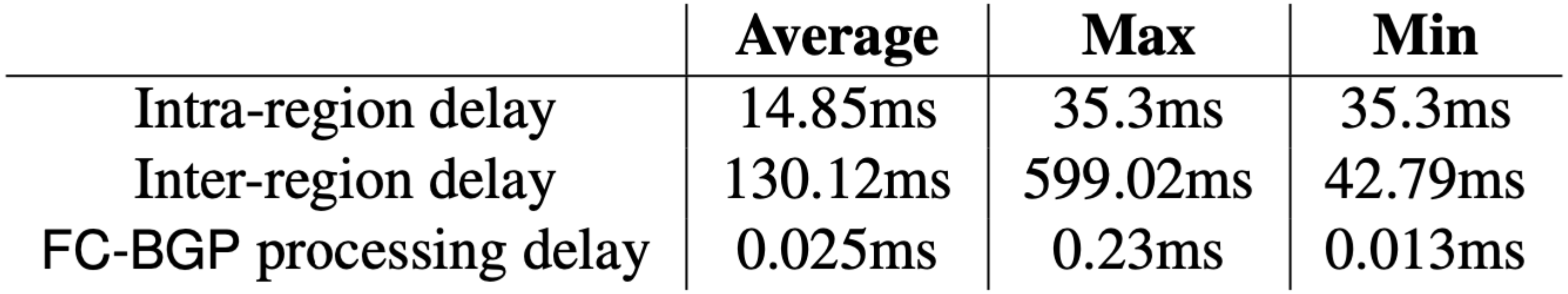
2. Hierarchical Topology on the Overlay Network



The network topology

We implement the control plane of FC-BGP based on Quagga (version 1.2.4), and then further build a global-scale testbed over the global cloud infrastructure to evaluate FC-BGP in the wild.



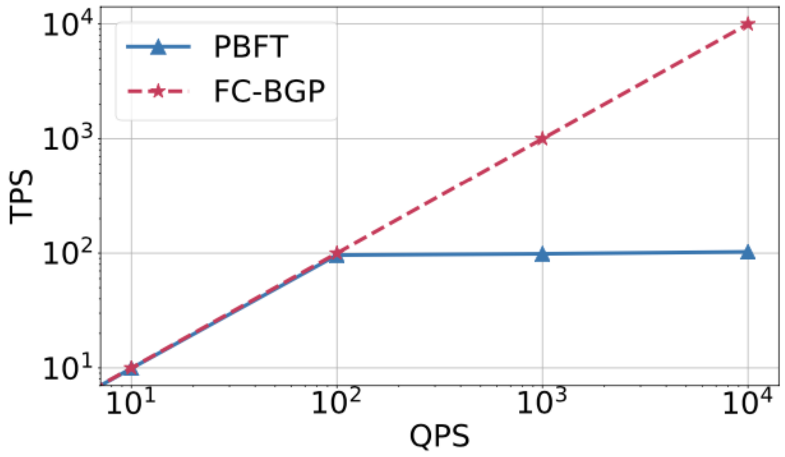


	Average	Max	Min
Intra-region delay	14.85ms	35.3ms	35.3ms
Inter-region delay	130.12ms	599.02ms	42.79ms
FC-BGP processing delay	0.025ms	0.23ms	0.013ms

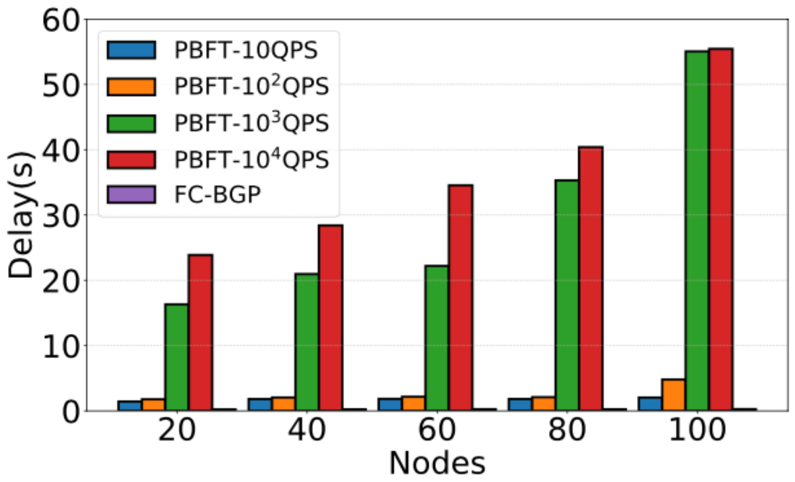
FC-BGP processing delays are minor

Evaluation

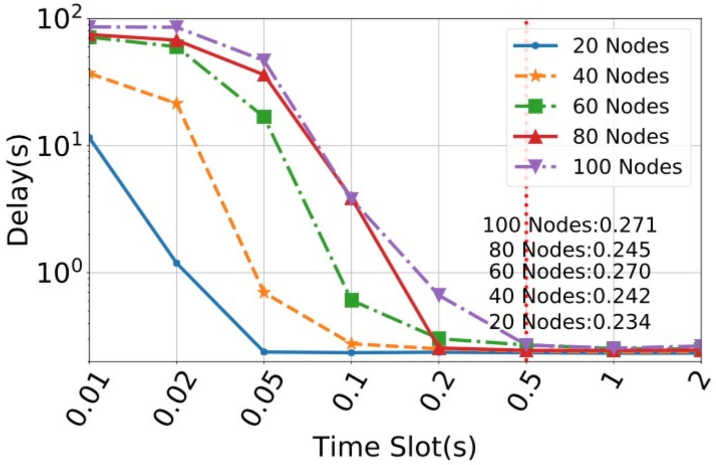
3. Data plane Validation Overhead



Throughput



Delay



Stability

- FC-BGP has roughly 100 times the throughput capacity of PBFT
- The consensus latency of PBFT is about 7 to 20 times that of FC-BGP
- For the 100- AS network, FC-BGP is stable as long as the consistency check period is greater than 0.5 second

Conclusion

✓ FC-BGP is the first secure inter-domain routing system that can simultaneously authenticate BGP routing updates and validate data plane forwarding in an efficient and incrementally-deployable manner.

✓ FC-BGP is built upon a unified primitive, named Forwarding Commitment, to enhance the security of control plane routing and data plane forwarding.

✓ FC-BGP saves roughly 55% of the overhead required to validate BGP announcements compared with BGPsec, and meanwhile, FC-BGP introduces a small overhead for building a globally-consistent view of the desirable forwarding paths.

See more details: *https://datatracker.ietf.org/doc/draft-wang-sidrops-fcbgp-framework/*
More planned drafts to be released at IETF 118 meeting

Thanks!