# Efficient Secure BGP AS Path using **FS-BGP**

Xia Yin, ***Yang Xiang***, Zhiliang Wang, Jianping Wu
Tsinghua University, Beijing

81th IETF @ Quebec

# Outline

- **Introduction**
  - **FS-BGP: Fast Secure BGP**
  - **Terminology**
  - **Quick review of S-BGP**
- FS-BGP
- Evaluation
- Discussion

# FS-BGP: **F**ast **S**ecure BGP

- How to secure the path
  - CSA (**Critical path Segment Attestation**) to secure the AS path
  - SPP (**Suppressed Path Padding**) to protect the optimal path and prevent effective hijacking
- Security
  - All the authenticated paths are **feasible path**
  - Achieves **similar level of security as S-BGP**
- Computational cost (on backbone router)
  - Singing cost: **~0.6%** of S-BGP
  - Verification cost: **~3.9%** of S-BGP

# Terminology (1)

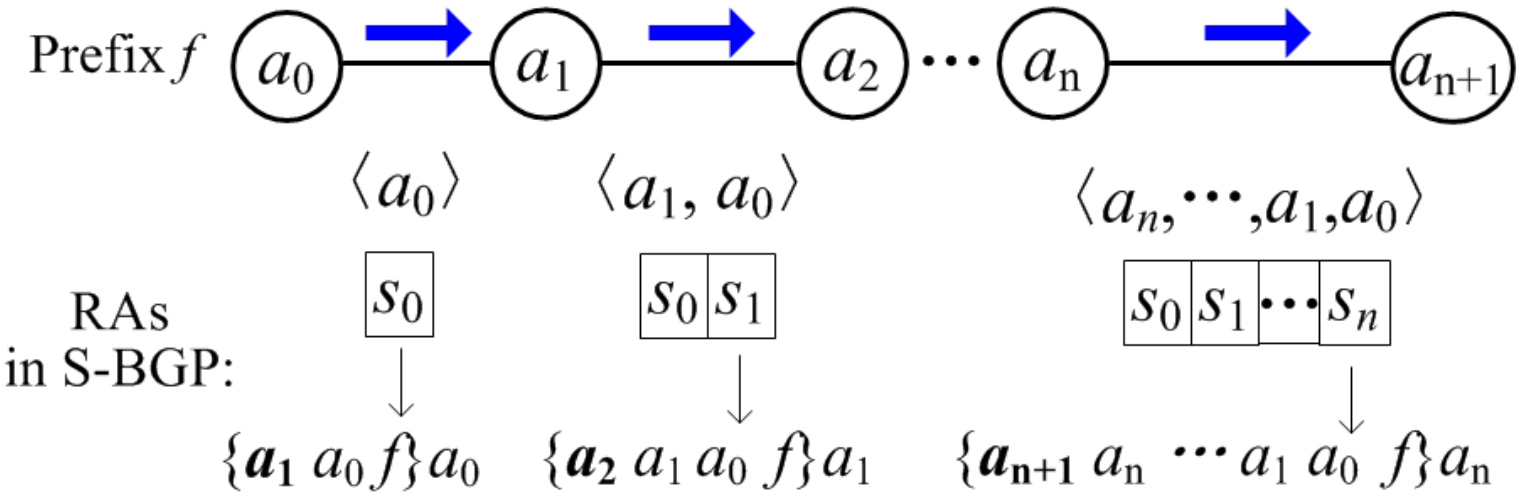
- Feasible Path
  - Exist in the AS-level graph, and satisfies **import and export policies** of all ASes along the path
- Unfeasible Path
  - (1) Paths do **NOT** exist in the DAG
  - (2) Paths **violate import and export routing policies**

# Terminology (2)

- Three categories of Feasible Path
  - **Outdated Path**: path announced but temporarily not available
  - **Current Path**: currently using and announcing path
  - Not announced Path: feasible but not announced, because BGP only announce the current optimal path each time

# Signatures in S-BGP

- Route Attestations (RA) to secure the path



# Pros and Cons of S-BGP

- Actually singed the whole path, including the recipient AS
- **Pros**: the most secure schema
- **Cons**
  - Unbearable computational cost, so many paths.
  - Long Exp-date: unable to defend replay attack
  - Short Exp-date: destroy the whole system

# Outline

- Introduction
- **FS-BGP: Fast Secure BGP**
  - **CSA: Critical Segment Attestation**
  - SPP: Suppressed Path Padding
- Evaluation
- Discussion

# Announcement Restrictions in BGP

- Best route announcing
  - **Temporary** restriction
  - Local preference and other metrics
- Selective import & export policy
  - **Persistent** restriction
  - ***Neighbor based import and export***: contracts ($$) are between neighbor Ases
  - Feasible path: exist in AS-level graph & obey the policy

# Critical Path Segment

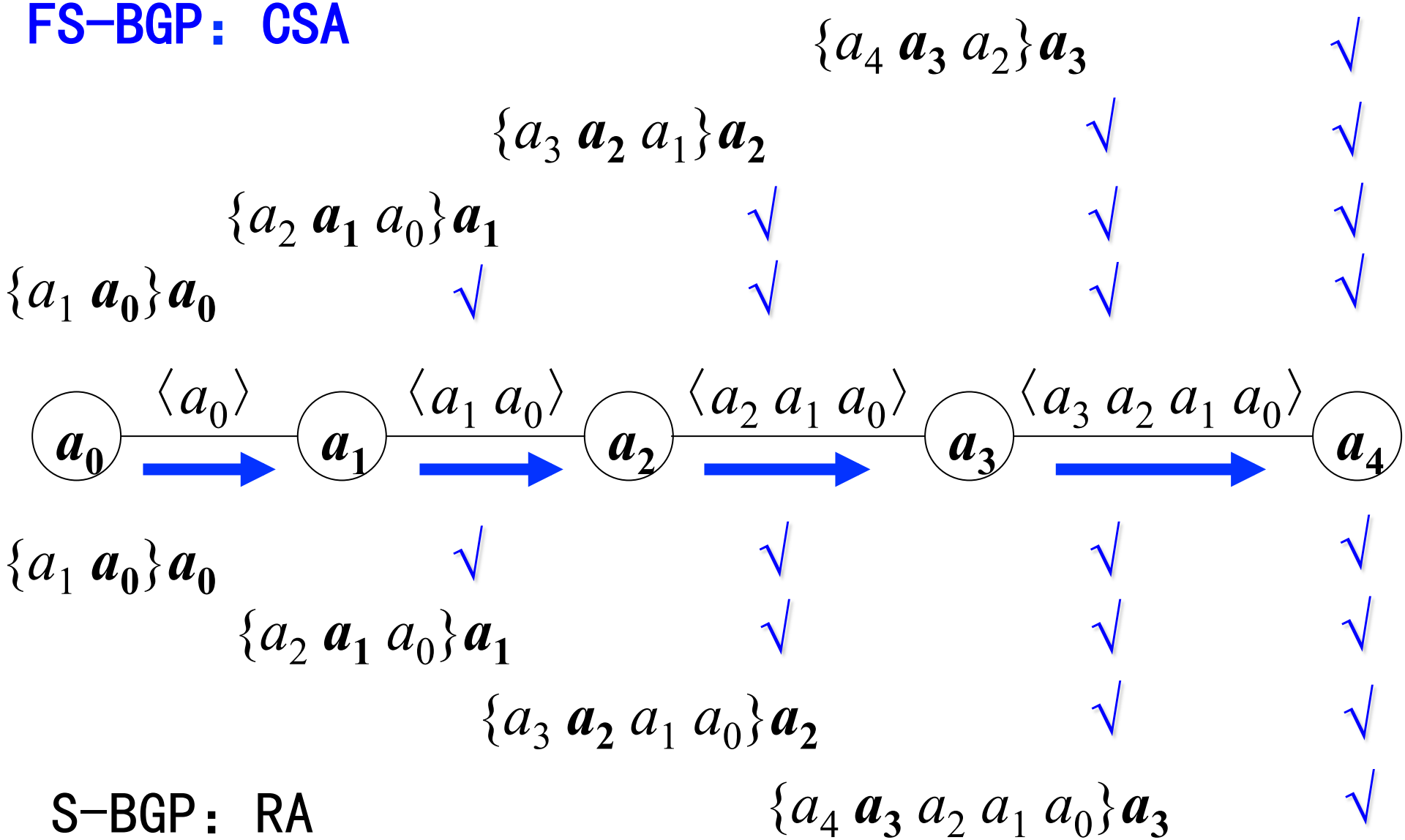
- In path: $p_n$ = <$a_{n+1}$ , $a_n$ , …, $a_0$>, the Critical Path Segment $c_i$ owned by $a_i$ is

$$c_i = \begin{cases} \langle a_1, a_0 \rangle & \text{for } i = 0 \\ \langle a_{i+1}, a_i, a_{i-1} \rangle & \text{for } 0 < i \leq n \end{cases}$$

- Those adjacent AS triples actually describes part of routing policy of the corresponding owner
  - $c_i$=<$a_{i+1}$, $a_i$, $a_{i\text{-}1}$> means $a_i$ can (***and already***) announce routes to $a_{i+1}$ which are import from $a_{i\text{-}1}$
  - If every owner sings the critical segment in a current announcing path, the consequence ASes will be able to verify the whole path

$\{msg\}a_i$: signature of $msg$ signed by $a_i$

**FS-BGP: CSA**

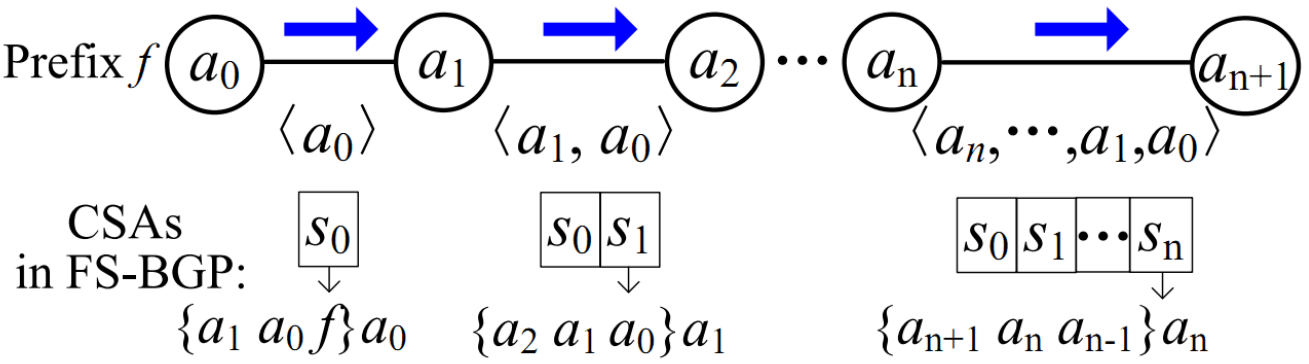



S-BGP: RA

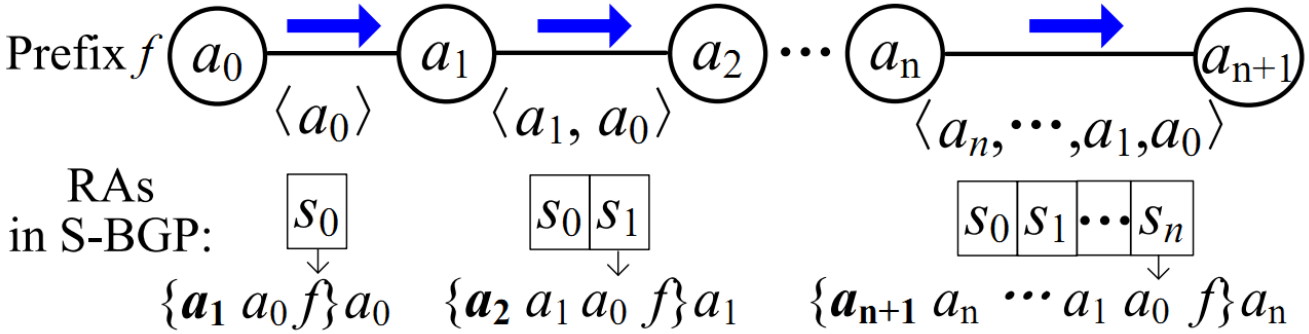
# Signatures in FS-BGP and S-BGP

**Signatures for the path: $p_n$=<$a_{n+1}$, $a_n$, $a_{n-1}$, …, $a_0$>**

**FS-BGP**

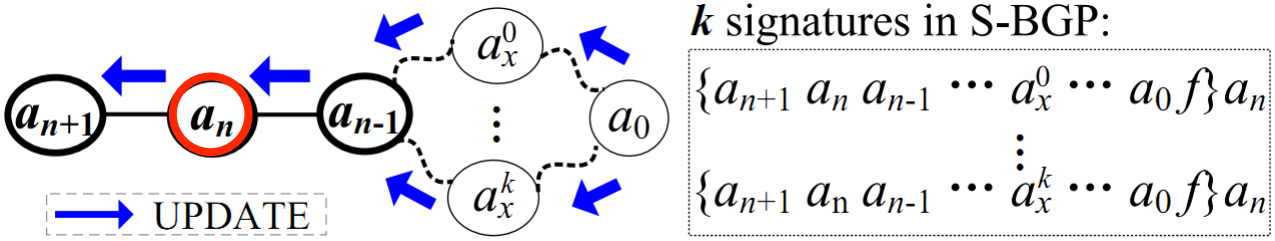



**S-BGP**



# Cost Reduction

- (# total critical segment) << (# total AS path)
- If we use a small cache, the cost will be sharply decreased




  - S-BGP: $a_n$ receives $k$ paths, signs ***k*** signatures
  - FS-BGP: $a_n$ receives $k$ paths, signs **1** signature

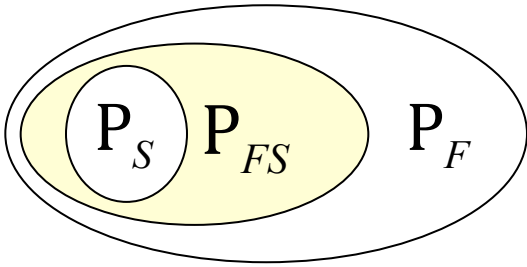
# Outline

- Introduction
- **FS-BGP: Fast Secure BGP**
  - CSA: Critical Segment Attestation
  - **SPP: Suppressed Path Padding (Optional)**
- Evaluation
- Discussion

# CSA achieves Feasible Path Authentication

- Paths can be verified in FS-BGP are all feasible paths [Theorem 1]

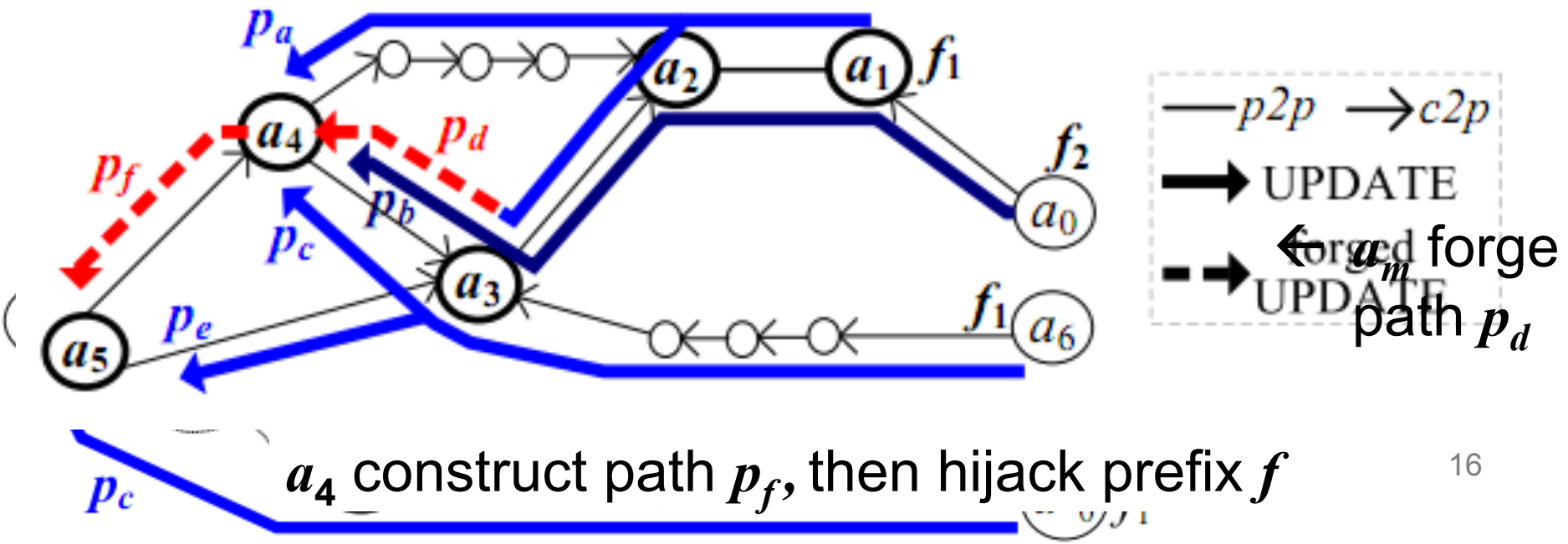
| Signed paths in S-BGP | | Signed paths in FS-BGP | | All feasible paths |
|---|---|---|---|---|
| $P_S$ | $\subset$ | $P_{FS}$ | $\subset$ | $P_F$ |




| | | |
|---|---|---|
| **1. Outdated path** | **1. Outdated path** | **1. Outdated path** |
| **2. Current path** | **2. Current path** | **2. Current path** |
| | **3. Revealed path** | **3. All not announced path** |

# Forge a path in FS-BGP is possible

- **Forged path** (**Revealed path**) in FS-BGP
  - Using authenticated path segments, manipulator can construct forged path, which is feasible but currently not announced.




$a_4$ construct path $p_f$, then hijack prefix $f$

# Conditions of **Effective Hijacking**

- **Effective hijacking**: the traffic is not forwarded by the attacker under normal status.
- (1) Forged path is **still feasible**, and only temporarily not received by the attacker!
- (2) Forge a path in FS-BGP is **very difficult**
  - Must be constructed using received authenticated path segments
  - Must not be announced by the intermediate AS
  - Can NOT be shorter than 5 hops [Theorem 2]
- (3) Only **short enough forge-path** can be used for a effective hijacking [Theorem 3]

# Prevent Effective Hijacking

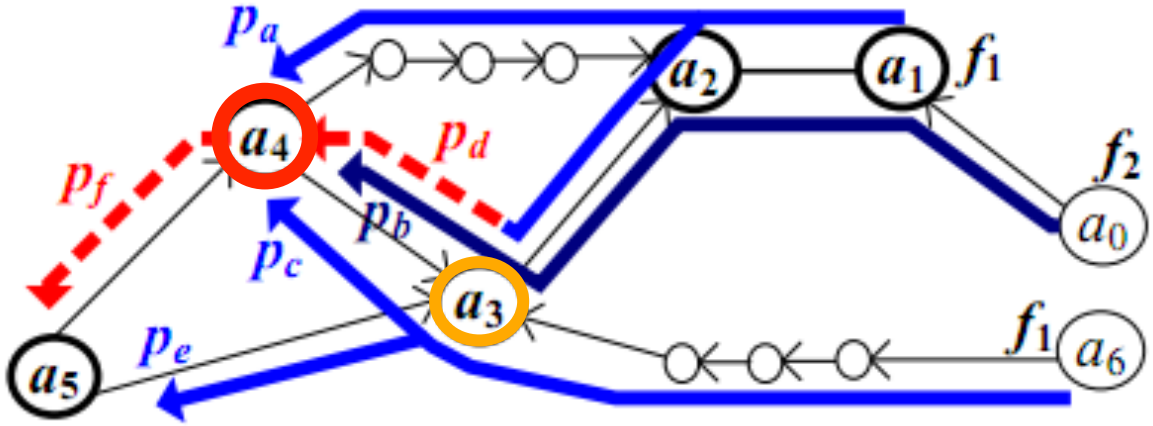
- Using ASPP, can grantee that attacker can not concatenate short enough forge path
- **Short enough**: shorter than the optimal path (longest live-time)

$\{a_4, a_3, a_2\}a_3$

↓

$\{a_4, a_3, 3, a_2\}a_3$

$p_f$=<$a_5$, $a_4$, $a_3$, $a_3$, $a_3$, $a_2$, $a_1$>



# SPP: Suppressed Path Padding

- Suppressed Path: paths with lower local preference in the decision process
- Suppressed path may shorter than optimal path

**Basic decision process:**

1. Highest Local Preference (LP)
2. Shortest Path Length (PL)
3. Tie Breaks (TB)

Compute $k_i$ :

**Algorithm 1** Suppressed Path Padding

**Input:** local AS $a$, neighbor AS $a$

**Output:** $k_i$:

padded ir

if $a_i = 1$ ha

return

$k_i \leftarrow 1$

for all pa

$opt(p)$ ·

if $PL($

$k_i \leftarrow$

return $k_i$

**Path categories:**

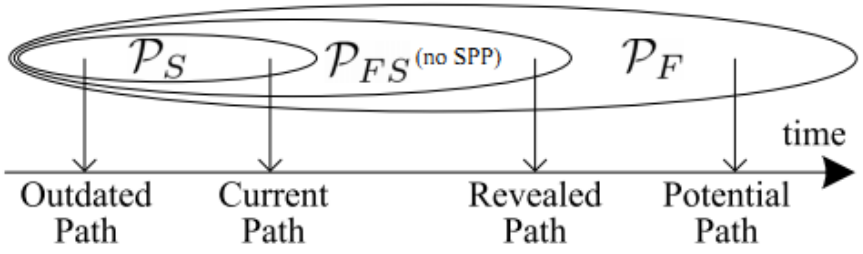
1. Suppressed Path
2. Sub-optimal Path
3. Optimal Path

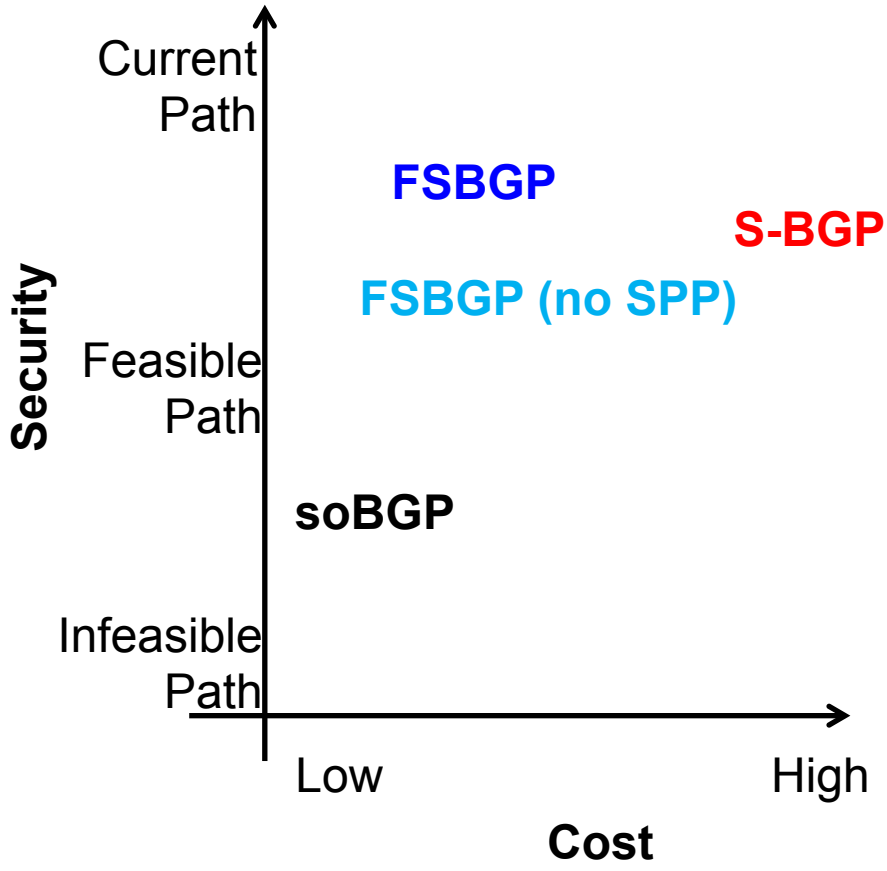
# Outline

- Introduction
- FS-BGP: Fast Secure BGP
- **Evaluation**
  - **Security Level**
  - **Computational Cost**
- Discussion

# Security Level

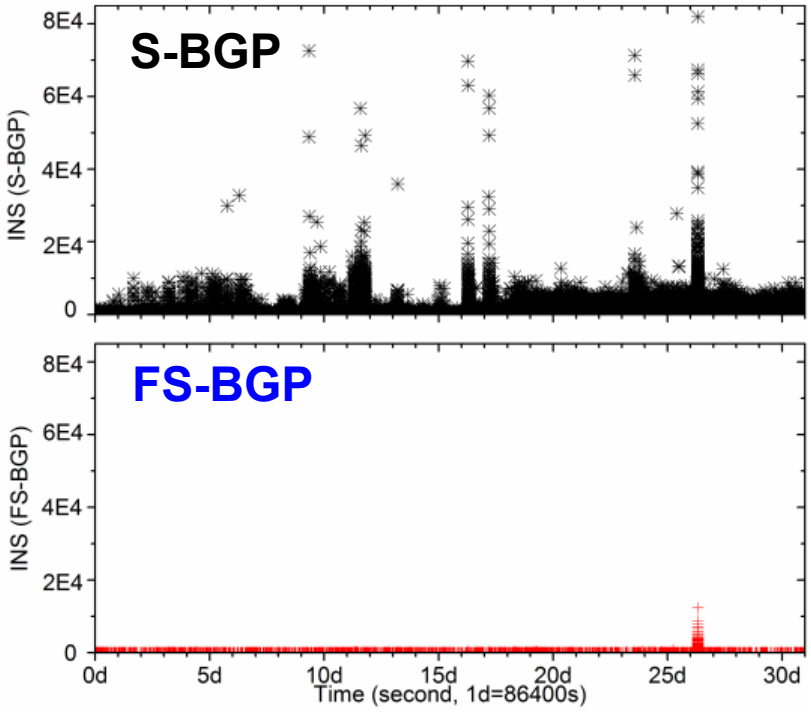
| Type of Attack | FS-BGP | S-BGP | FS-BGP (no SPP) | so BGP |
|---|---|---|---|---|
| Inefficient hijack | √ | √ | √ | √ |
| False origin AS | √ | √ | √ | √ |
| Infeasible path | √ | √ | √ | × |
| Feasible path | | | | |
| Potential path | √ | √ | √ | × |
| Revealed path | √* | √ | × | × |
| Outdated path | √* | × | × | × |
| Policy violating [10] | × | × | × | × |
| Link-cut [4] | × | × | × | × |



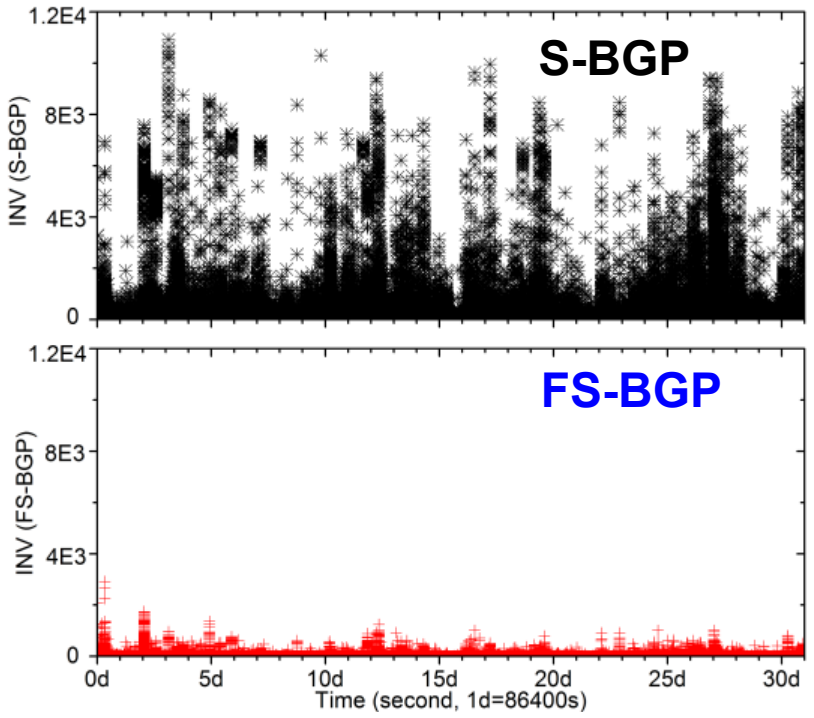



# Computational Cost

- 30 days' real BGP updates from backbone routers




**# signings in every second**




**# verifications in every second**

# Outline

- Introduction
- FS-BGP: Fast Secure BGP
- Evaluation
- **Discussion**
  - **Support complicated routing policies**
  - **Protect privacy**

# Complicated Routing Policies

- AS may use complicate route filters to describe their routing policies
  - Prefix filter:
  - Path filter:
  - Origin filter:

| | |
|---|---|
| *export*: *to* AS1 *announce* RS-ABC<br>*export*: *to* AS2 *announce* 213.153.0.0/19<br>*export*: *to* AS3 *announce* AS3^16-24 | ← Included feasible prefixes into CSA |
| *export*: *to* AS4 *announce* <^AS4$> | ← Sign whole path |
| *export*: *to* AS5 *announce* AS-EFG<br>*export*: *to* AS6 *announce* AS6 | ← Included feasible origins into CSA |

- FS-BGP can flexibly support route filters

# Revisit the route filters

- Quantity of route filter
  - According our statistical result in IRR database, **only a very small portion** of policies use route filters
- Purpose of route filter
  - Some (i.e., origin/path filter) are set for **security considerations**, rather than policy requirements.
  - Others (i.e., prefix filter) are set for traffic engineering, to identifying the **preference of a route**, rather than the feasibility of a path

# Privacy Protection

- Privacy: customer list …
- FS-BGP can protect privacy data
  - Message spreading manner is same to BGP
  - Path segments not reveal additional info.
  - Path segments can only be passively received by valid BGP UPDATE receivers
  - Do NOT offer any kinds of public accessible policy database

# Next step: call for **WG adoption**

- Acknowledgement
  - Greatly appreciate comments of ***Russ White***
- Review
  - FS-BGP: Fast Secure BGP
    - CSA: Critical Segment Attestation
    - SPP: Suppressed Path Padding (Optional)
  - Evaluation
    - Security level: **similar security level as S-BGP**
    - Computational cost: **reduced the cost by orders of magnitude**
    - Support complicated routing policies
    - Protect privacy

**Thanks!**