Transitive BGPsec is Difficult/Infeasible

https://datatracker.ietf.org/doc/draft-wang-sidrops-bgpsec-transition/

Zhuotao Liu

Authors: Ke Xu, Xiaoliang Wang, Zhutao Liu, Qi Li, and Yangfei Guo

SIDROPS WG
IETF 123
Jul. 2025

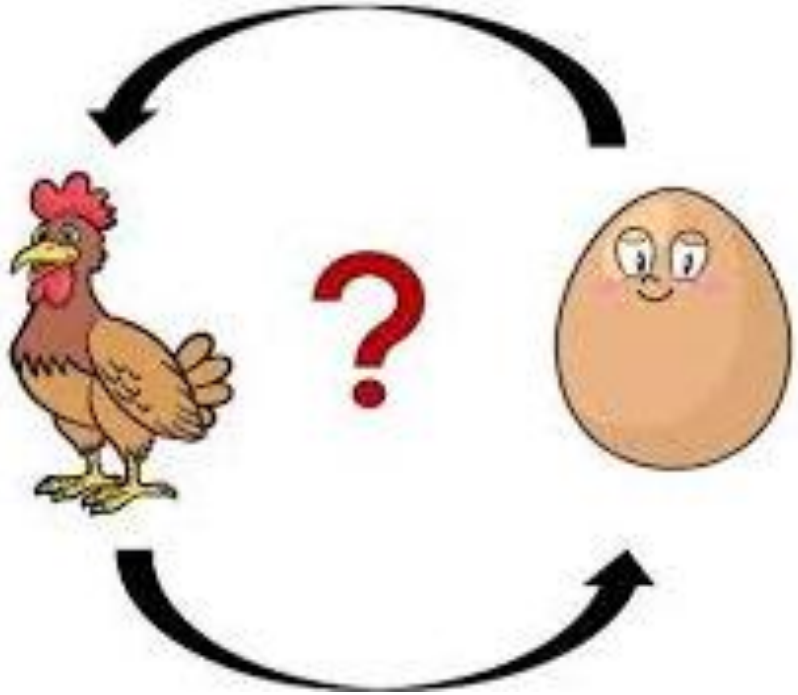
Motivation

- The BGPsec protocol experiences very limited attention in case of deployment
  - Only one BGPsec public key is available in RPKI as of Jun. 3, 2025.
    - https://console.rpki-client.org/rpki.json
- Barriers
  - OPEN Negotiation
    - BGPsec Capability
    - Multiprotocol Capability
  - UPDATE
    - non-transitive
  - Incentives for early adopters
- **Goal**: Can we make BGPsec transitive to facilitate the deployment of BGPsec?


```
"metadata": {
        "buildmachine": "dus-vrp-gen1.rpki-client.org",
        "buildtime": "2025-06-03T06:03:05Z",
        "elapsedtime": 841,
        "usertime": 1139,
        "systemtime": 1584,
        "roas": 305389,
        "failedroas": 18,
        "invalidroas": 0,
        "spls": 1,
        "failedspls": 1,
        "invalidspls": 0,
        "aspas": 88,
        "failedaspas": 1,
        "invalidaspas": 0,
        "bgpsec_pubkeys": 1,
        "certificates": 46892,
        "invalidcertificates": 14,
        "nonfunctionalcas": 168,
        "taks": 0,
        "tals": 5,
        "invalidtals": 0,
        "talfiles": [
                "/etc/rpki/afrinic.tal",
                "/etc/rpki/apnic.tal",
                "/etc/rpki/lacnic.tal",
                "/etc/rpki/ripe.tal",
                "/etc/rpki/arin.tal"
        ],
        "manifests": 46878,
        "failedmanifests": 168,
        "crls": 46710,
        "gbrs": 2,
        "repositories": 100,
        "vrps": 712414,
        "uniquevrps": 700659,
        "vsps": 0,
```

Motivation (Cont.)

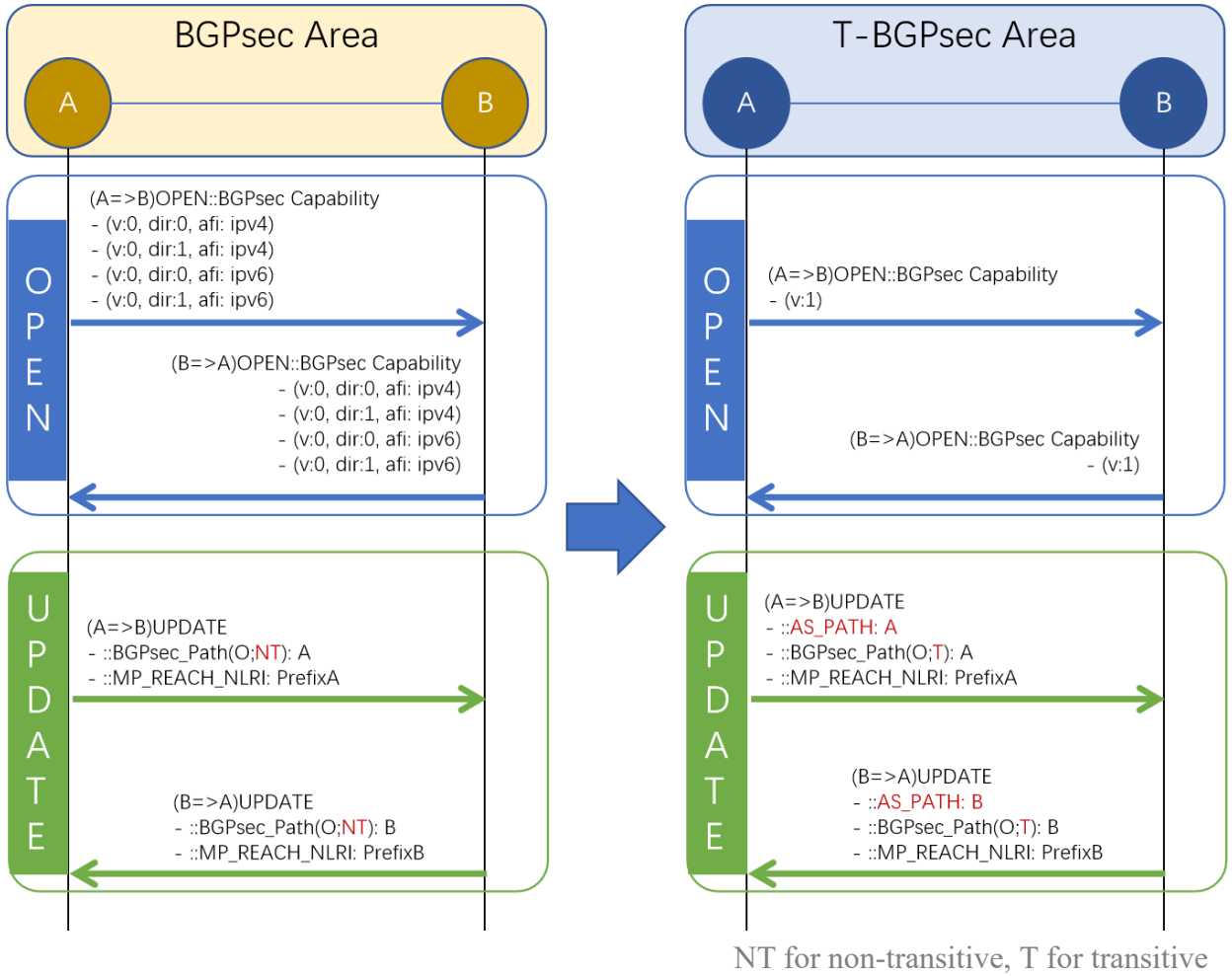
- Chicken-and-Egg Problem
  - The design of BGPsec prioritizes technology over deployer preference.
  - There are fewer incentives for early adopters in today's routing security mechanisms.[1]
  - If there are no benefits to the early adopters, why become early adopters in the first place?
- A Desirable Secure BGP Mechanism
  - Incremental deployability should allow early adopters to benefit, avoiding the chicken-and-egg problem.



[1] NTIA Supports FCC Internet Routing Security Proposal. https://www.ntia.gov/press-release/2024/ntia-supports-fcc-internet-routing-security-proposal.

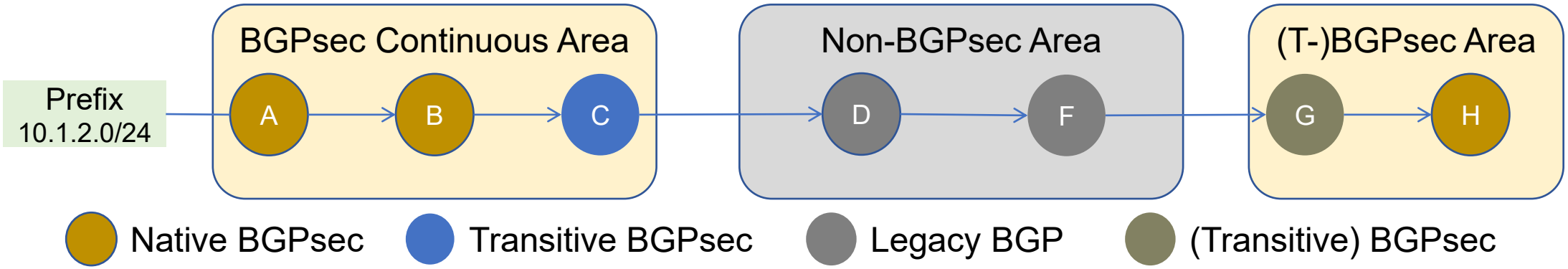
Overview: Transitive BGPsec

- **Packet formats of BGPsec are reused**
- BGP Open::BGPsec Capability
  - Version is upgraded
- BGP Update
  - AS_PATH is reserved
  - BGPsec_PATH: non-transitive => transitive
- Signature Choices
  - Onion-like signature (all ASes on the current path are involved in a signature)
  - Pathlet signature (only previous ASN, local ASN, next ASN are involved in a signature)
- Questions
  - Compatibility with Native BGPsec



NT for non-transitive, T for transitive

Q: Compatibility with Native BGPsec



- BGP route propagation
  - AS A=>B: BGPsec UPDATE<P; BGPsec_Path{AS_A, SIG_{AB}}>
  - AS B=>C: BGPsec UPDATE<P; BGPsec_Path{AS_B, AS_A, SIG_{BC}, SIG_{AB}}>
  - AS C=>D: BGP UPDATE<P; AS_PATH{AS_C, AS_B, AS_A}, BGPsec_PATH{AS_B, AS_A, SIG_{BC}, SIG_{AB}}>
  - AS D=>F: BGP UPDATE<P; AS_PATH{AS_D, AS_C, AS_B, AS_A}, BGPsec_PATH{AS_B, AS_A, SIG_{BC}, SIG_{AB}}>
  - AS F=>G: BGP UPDATE<P; AS_PATH{AS_F, AS_D, AS_C, AS_B, AS_A}, BGPsec_PATH{AS_B, AS_A, SIG_{BC}, SIG_{AB}}>
- If AS G deploys Transitive BGPsec
  - AS G=>H: BGPsec UPDATE<P; BGPsec_PATH{AS_G, AS_F, AS_D, AS_C, AS_B, AS_A, SIG_{GH}, SIG_{BC}, SIG_{AB}}
    - But, downgrading to BGP may be a better choice for AS G, as it knows AS H only supports BGPsec.
- If AS G deploys Native BGPsec
  - The verification result of BGPsec_PATH is INVALID at AS G.

Conclusion

- It is difficult/infeasible to render BGPsec as a transitive approach for traversing undeployment areas while:
  - still using BGPsec_PATH type code in BGP UPDATE message,
  - and maintaining compatibility with native BGPsec.

We probably need a new optional, transitive path attribute so that it will not confuse with the BGPsec_PATH.

A bigger question: what should we, as a community, do to secure BGP paths?

Thank you!

IETF 123 SIDROPS

Jul. 2025