Forwarding Commitment BGP Testbed and Deployment Experience

Tsinghua University & Zhongguancun Laboratory

Ke Xu, Xiaoliang Wang, Zhuotao Liu, Qi Li, Ziwei Li, Yangfei Guo, Jianping Wu

Nov. 2025

Key Points of FC-BGP

Goals and Challenges

- FC-BGP aims to authenticate BGP route announcements by introducing cryptographic assurances for AS_PATH attributes.
- A significant challenge is ensuring security in scenarios where not all ASes have adopted FC-BGP, necessitating compatibility with existing BGP protocols.

Core Mechanism

- FC-BGP introduces an optional, transitive path attribute called the Forwarding Commitment (FC), which is a cryptographically signed segment certifying an AS's routing intent on its directly connected hops.

Compared to BGPsec

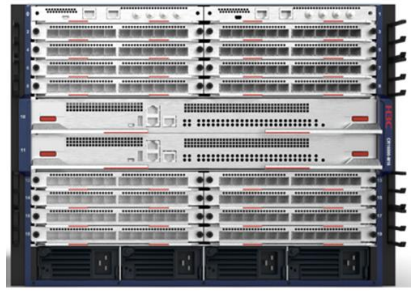
- FC-BGP offers a different security guarantee with transitive Path Attribute, ensuring AS-PATH validation while maintaining compatibility in partial deployment scenarios.

Deployment Motivation

中国电信 CHINA TELECOM

清華大學 Tsinghua University

H3C



CR16000 Router

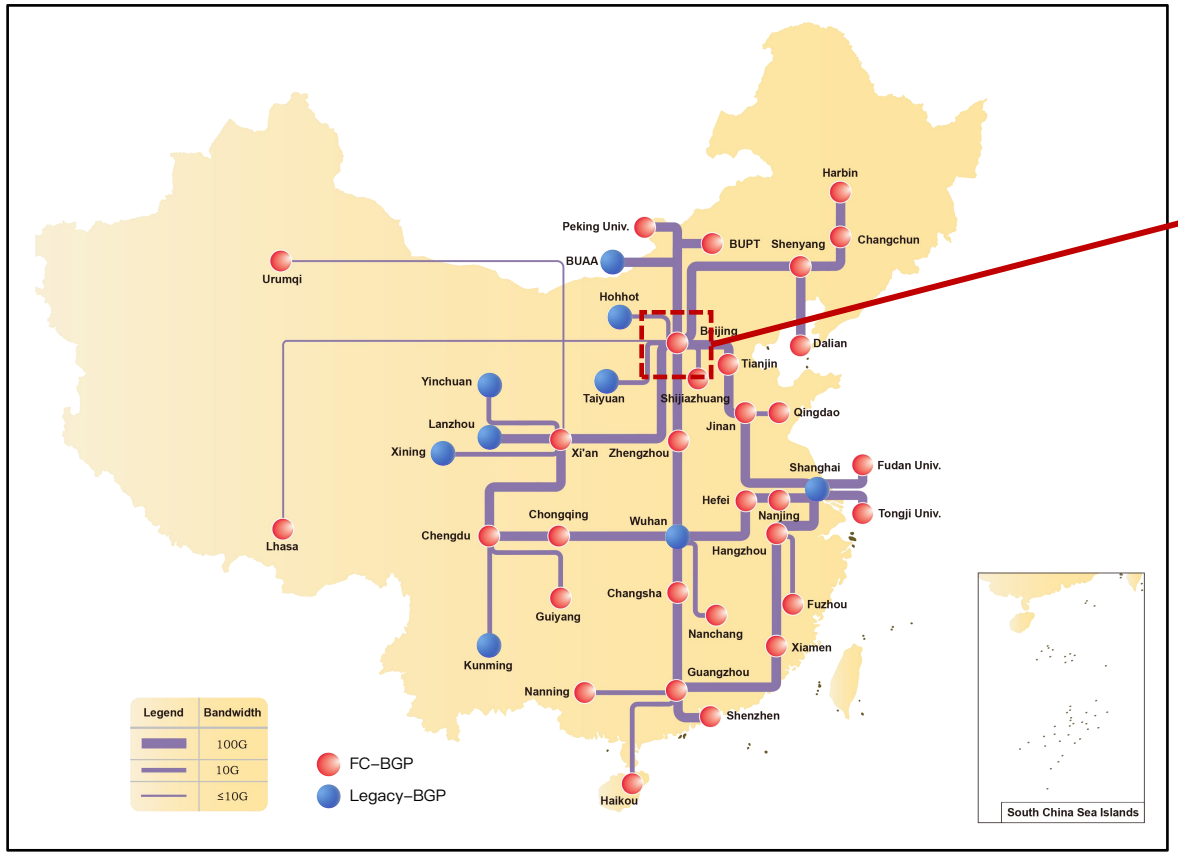
CR19000 Router

Commercial Development and Upgrade

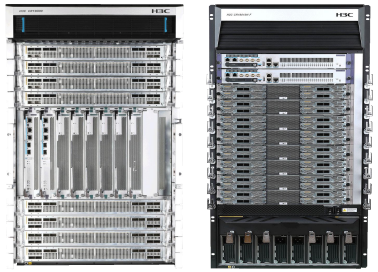
A real-time warning platform for routing anti-hijacking and anti-leakage, co-developed by China Telecom and Tsinghua University, has issued alerts on numerous routing hijacking and leakage events.

Therefore, H3C, in collaboration with China Telecom and Tsinghua University, has implemented commercial upgrades to its CR16000 and CR19000 routers to support FC-BGP. This enhancement is intended to improve inter-domain routing security.

Progress in Deployment



FITI Backbone Node Device

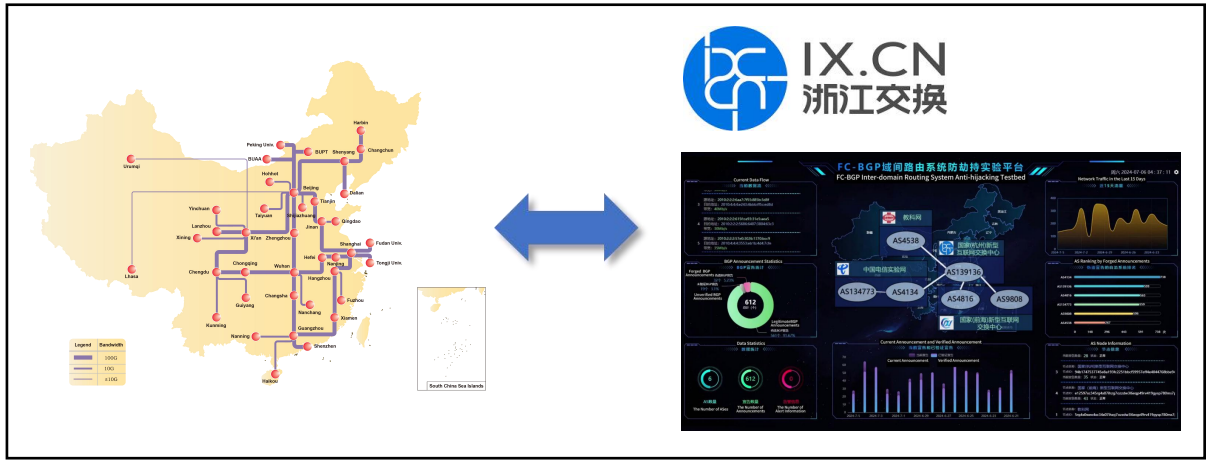


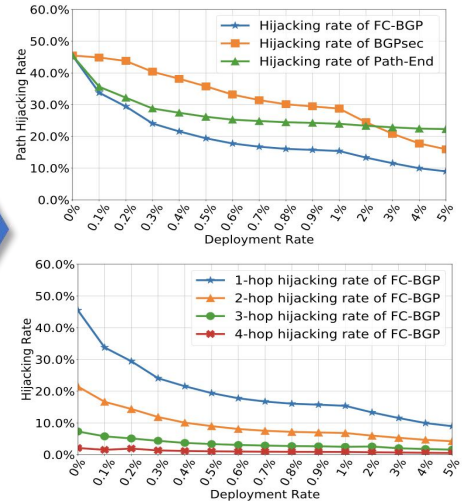
H3C CR16000/19000

FITI holds 4096 ASN assigned by APNIC, along with a /20 IPv6 address block. With sites distributed across China, it features a genuine internet environment suitable for large-scale network experimentation, with a maximum bandwidth of up to 1.2T.

Future Internet Technology Infrastructure, **FITI**

Progress in Deployment





BGP topology and announcement datasets

Testbed for FC–BGP (FITI and IXPs)

Security Benefits in Partial Deployment

Utilizing public datasets from RouteViews, we performed Internet BGP topology reconstruction and BGP announcement replay on the Testbed. Simultaneously, we adjusted the deployment ratio of FC–BGP to calculate the network–wide route hijackability rate under partial deployment scenarios as the deployment rate increases.

Test Experience and Results

Functional Test

- FC-BGP prototype correctly implemented the functionalities as defined in the FC-BGP protocol specification.

Partial Deployment Test

- FC-BGP works reliably in mixed environments. Legacy routers (Huawei, H3C, etc.) transparently forward UPDATEs with FC attributes, preserving message integrity. Results confirm incremental deployability and better security than BGPsec in partial deployment.

Key takeaways

- The FC-BGP prototype handles both IPv4 and IPv6 routing correctly. It functions properly as a BGP route reflector and client, interoperating with commercial routers from multiple vendors.

Conclusion

- FC–BGP offers efficient and scalable AS path verification while preserving compatibility and stability with existing routing protocols. These advantages are achieved without the need for modifications to the current Internet architecture.

- Incremental deployment is a key design principle that was used in the experiment. The results indicate that, even with partial deployment, FC–BGP provides significant security benefits in protecting routing information, encouraging early adoption of the solution by service providers.

Thank You!

https://datatracker.ietf.org/doc/draft-li-sidrops-fcbgp-experiment/