Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 12 December 2025

K. Xu
X. Wang
Z. Liu
Q. Li
J. Wu
Tsinghua University
Z. Li
Y. Guo
Zhongguancun Laboratory

10 June 2025

Forwarding Commitment BGP Testbed and Deployment Experience
draft-li-sidrops-fcbgp-experiment-00

Abstract

Forwarding Commitment BGP (FC-BGP) enables the establishment of a secure inter-domain routing system by providing security for the path of Autonomous Systems (ASs) through which a BGP UPDATE message passes. In an effort to enhance the validation of FC-BGP, a prototype implementation of the FC-BGP was developed and an evaluation was conducted on the FITI high-performance IPv6 backbone network. This document reports on the prototype implementation and the results of the evaluation.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://FCBGP.github.io/FCBGP-experiment/draft-li-fcbgp-experiment.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-li-sidrops-fcbgp-experiment/.

Source for this draft and an issue tracker can be found at https://github.com/FCBGP/FCBGP-experiment.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

The current inter-domain routing system lacks a mechanism in BGP to ensure the authenticity of path attributes announced by an Autonomous System (AS). This deficiency exposes a broad attack surface and enables risks such as traffic interception, denial-of-service, and man-in-the-middle attacks[RFC4272].Forwarding Commitment BGP (FC-BGP) is a novel forwarding-path verification framework designed to address these security challenges inherent in today’s inter-domain routing system. By introducing a Forwarding Commitment (FC), FC-BGP offers a solution that integrates seamlessly with the existing routing infrastructure. Through the use of FCs to provide a verifiable view of routing intent, FC-BGP ensures that the actual forwarding path conforms to declared routing policies.

As part of the development of the Forwarding Commitment BGP (FC-BGP) framework, we implemented a FC-BGP prototype and deployed the prototype in the operational networks of 40 Autonomous Systems (ASes) within the Future Internet Technology Infrastructure (FITI). The evaluation demonstrates that FC-BGP achieves significant performance improvements in large-scale network deployments and that even limited deployment yields substantial security benefits. This document first describes a FC-BGP prototype solution, then outlines the experimental environment, and finally presents the experimental results. It is anticipated that this document will provide useful insights for those interested in this subject and serve as preliminary input for future IETF work in this area.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. A Prototype FC-BGP Implementation

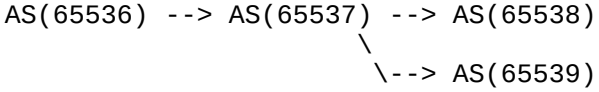


Figure 1: An FC-BGP UPDATE propagation example.

This section describes a prototype implementation of FC-BGP, using a simplified topology as illustrated in Figure 1. Only the essential operations are highlighted here; readers are referred to [FC-BGP-Protocol] for the complete protocol specification.

In this example, all Autonomous Systems (ASes) are standard ASes; Route Servers (RSes) and AS Confederations are not considered. Additionally, no AS Path Protection (ASPP) mechanisms are applied.

For the purposes of discussion, it is assumed that:

1. AS 65536 owns the prefix 192.0.2.0/24.

2. AS 65537 receives an FC-BGP UPDATE message for the prefix 192.0.2.0/24 from AS 65536.

3. AS 65537 then propagates the route to AS 65538 and AS 65539.

An FC-BGP speaker SHOULD propagate an FC-BGP UPDATE message to downstream ASs only after completing the validation and best route path selection.

3.1. FC Generation at the Originating AS

When preparing to propagate a route, the FC-BGP speaker in AS 65536 performs the following steps:

1. Constructs the FC segment:

   Sets the Previous AS Number (PASN) to 0 (NULL).

   Sets the Current AS Number (CASN) to 65536.

   Sets the Next AS Number (NASN) to 65537.

2. Computes the signature as follows: Signature=ECDSA(SHA256(PASN, CASN, NASN, Prefix, Prefix Length)).

3. Constructs the FC Path attribute by embedding the newly generated FC segment.

4. Encapsulates the route announcement in a BGP UPDATE message and transmits it to AS 65537.

3.2. FC Verification at the Receiving AS

Upon receiving the UPDATE message, the FC-BGP speaker in AS 65537:

1. Extracts the FC Path attribute.

2. Retrieves the list of FC segments.

3. Identifies the FC segment where CASN == 65536.

4. Verifies that:

   PASN == 0.

   NASN == 65537.

5. Retrieves the corresponding public key using the Subject Key Identifier (SKI) field.

6. Verifies the signature using the algorithm indicated by the Algorithm ID field.

If the signature matches, the AS hop from 65536 to 65537 is considered verified. This process repeats for each FC segment corresponding to the AS_PATH entries if applicable.

If AS 65537 does not support FC-BGP, its BGP speaker MUST propagate the UPDATE message without validating the FC Path attribute.

3.3. FC Generation at Intermediate ASes

An FC-BGP speaker MUST generate a distinct UPDATE message for each downstream neighbor. Each UPDATE message MUST announce only a single IP prefix and MUST NOT aggregate multiple prefixes.

This restriction is necessary because different prefixes may follow different routing policies, resulting in different Forwarding Commitments. Aggregating prefixes could cause errors in FC generation and validation.

Thus, AS 65537 generates:

An UPDATE message for AS 65538 with NASN set to 65538.

A separate UPDATE message for AS 65539 with NASN set to 65539.

For each UPDATE to a downstream neighbor (e.g., AS 65538), the FC-BGP speaker in AS 65537:

1. Encapsulates the route prefix into a single UPDATE message.

2. Constructs a new FC segment:

   Sets the Previous AS Number (PASN) to 65536.

   Sets the Current AS Number (CASN) to 65537.

   Sets the Next AS Number (NASN) to 65538.

Computes the SHA-256 digest over (PASN, CASN, NASN, IP Prefix Address, IP Prefix Length).

Signs the digest using ECDSA.

Fills in the Signature and other required FC fields.

3. Prepends the newly created FC segment to the existing FC List.

4. Completes the FC Path attribute.

5. Continues with standard BGP UPDATE processing and transmission.

4. FC-BGP Testbed

4.1. FITI

The prototypes of our solutions for FC-BGP are implemented and tested on Future Internet Technology Infrastructure(FITI). FITI is a major scientific and technological infrastructure project in China, constructed and operated by the National Development and Reform Commission, the Ministry of Education, Tsinghua University, and other participating universities. The FITI high-performance backbone network connects 40 universities across 35 cities in 31 provinces, autonomous regions, and municipalities, with backbone links supporting bandwidths of up to 1.2 Tbps. FITI has been assigned 4096 Autonomous System Numbers (ASNs) by APNIC, along with a 240a:a000::/20 IPv6 address block. With geographically distributed sites across China, FITI provides a genuine internet environment suitable for large-scale network experimentation.

4.2. FC-BGP Testbed on FITI Infrastructure

The FC-BGP testbed was deployed on the FITI backbone network, as illustrated in Figure 2. FITI provides a network environment comprising 40 interconnected ASes located in cities such as Beijing, Shanghai, Nanjing, and Shenzhen. These ASes are capable of running the BGP protocol, support customizable routing policies, and reflect realistic physical and geographical topologies. Each AS can host multiple routers. The FC-BGP mechanism was implemented in 31 of the ASes, including deployment on commercial H3C CR16000 or CR19000 routers in a subset of them. After software updates, these 31 ASes were fully FC-BGP-enabled, supporting route exchange as well as FC attribute transmission and reception. The remaining 9 ASes did not deploy FC-BGP and were used to construct a partial deployment scenario.The testbed is fully capable of supporting the evaluation requirements for the FC-BGP solution.

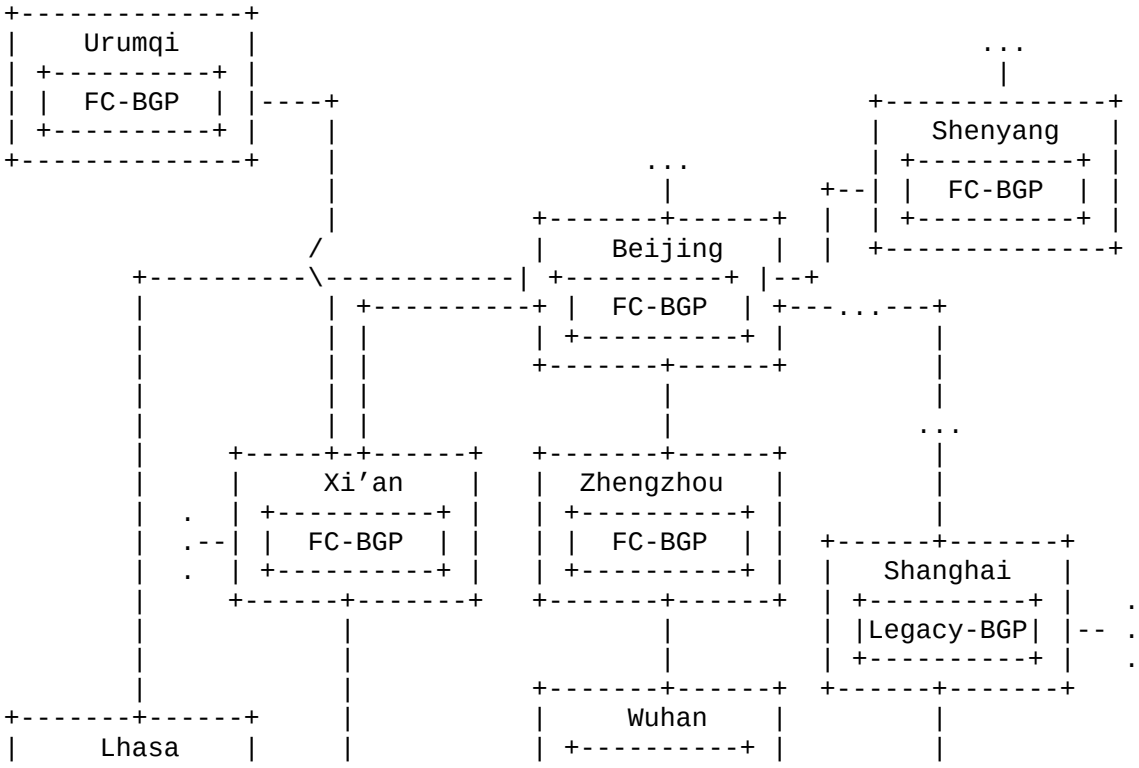
GitHub repository: https://github.com/fcbgp/fcbgp-implementation

5. Test Experience and Results

The prototype implementation of FC-BGP, as described in Section 2, was deployed on the testbed outlined in Section 3. The functionality of the FC-BGP prototype and its compatibility under partial deployment scenarios were evaluated. All features were successfully tested, as detailed in the experimental results presented in this section.

5.1. Test Experience

1. Functional testing of FC-BGP is conducted to verify the protocol's compliance with its specification in terms of message construction and operational behavior. The evaluation focuses on verifying that a BGP speaker is able to correctly construct BGP UPDATE messages containing the FC path attribute and that the message format conforms to the FC-BGP specification. In addition, the tests validate that the FC-BGP implementation correctly performs AS path validation procedures.



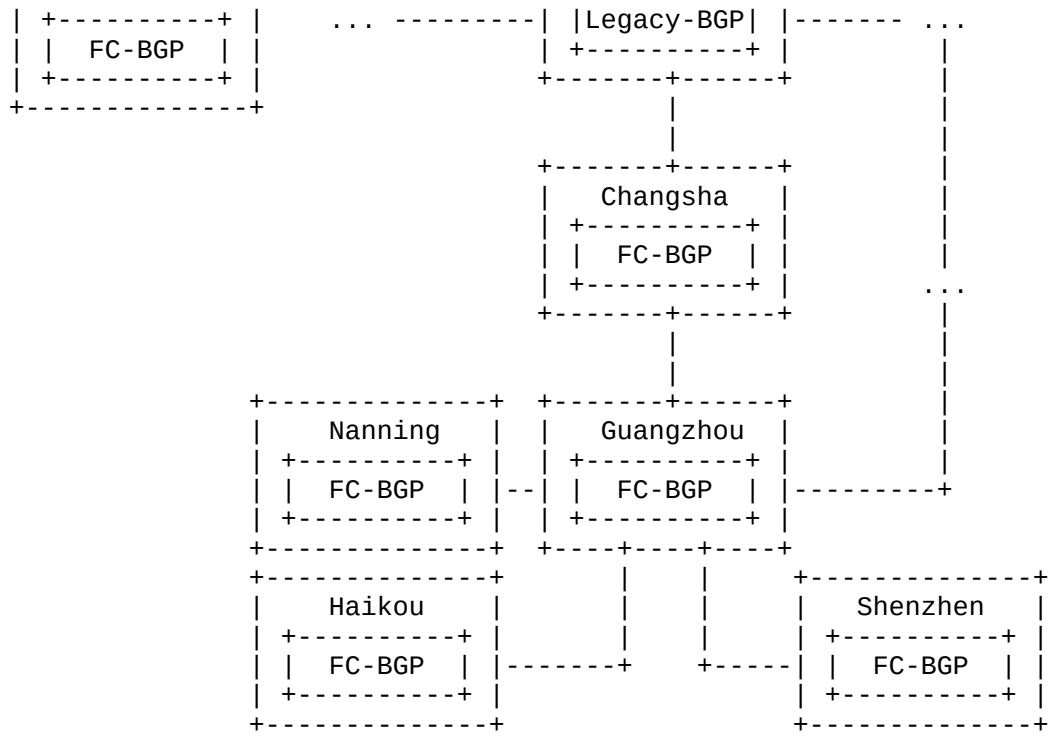


Figure 2: FC-BGP Testbed on FITI Infrastructure.

1. To assess the effectiveness and compatibility of FC-BGP in partial deployment scenarios, a testbed is constructed consisting of routers that support the FC-BGP mechanism and intermediate routers that do not support it. The goal of the testing is to confirm that routers without FC-BGP mechanism support can transparently forward BGP UPDATE messages containing FC path attributes without discarding or altering them. This ensures that FC path attributes are preserved even when traversing BGP routers that do not support the FC-BGP mechanism.

2. Evaluate the compatibility of the FC-BGP prototype device in a variety of network scenarios. Verify the routing processing capabilities of the FC-BGP device under different address families, including IPv4 and IPv6. Test the compatibility of the FC-BGP prototype device, when functioning as a BGP route reflector (RR) and RR client, in networks composed of commercial routers from different vendors.

5.2. Test Results

1. The test results indicated that the FC-BGP prototype correctly implemented the functionalities as defined in the protocol specification [FC-BGP-Protocol]. All FC-BGP-enabled BGP speakers were able to successfully generate FC-BGP UPDATE messages that conformed to the protocol specification, and the receiving AS was able to correctly perform the path validation procedure. The FC path validation mechanism functioned as intended, verifying each hop in the AS_PATH sequentially. In scenarios where the receiving AS did not support FC-BGP, the system was still able to forward FC-BGP UPDATE messages without disruption.

2. Under partial deployment conditions, FC-BGP demonstrated good compatibility with legacy BGP routers. Commercial routers from different vendors that do not support FC-BGP (such as Huawei and Ruijie) were able to transparently forward UPDATE messages containing FC path attributes, and the integrity of these messages was preserved throughout the forwarding process. These results suggest that FC-BGP supports incremental deployment and remains compatible with existing BGP implementations. With respect to partial deployment, Section 5.1.1 of [FC-ARXIV] demonstrates that an adversary cannot forge a valid AS path when FC-BGP is fully deployed. Furthermore, Section 5.1.2 of [FC-ARXIV] analyzes the advantages of FC-BGP in partial deployment scenarios. The analysis shows that FC-BGP offers greater security benefits than BGPsec under partial deployment conditions.

3. The test results indicated that the FC-BGP prototype device was capable of correctly receiving and processing routing information for all supported address families. When operating as a BGP RR, the FC-BGP prototype device correctly reflected both IPv4 and IPv6 routes to its clients. Additionally, when acting as a BGP RR client, the FC-BGP prototype device was able to properly receive routes from the RR. These results demonstrate that the FC-BGP prototype device exhibits strong compatibility across a variety of network scenarios.

6. Conclusion

In conclusion, experimental results demonstrate that:

1. 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.

2. 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.

7. Security Considerations

The purpose of this document is to report FC-BGP testbed and experimental results. Security considerations related to the solution mechanisms are discussed in [FC-BGP-Protocol] and [FC-ARXIV] for details.

8. IANA Considerations

This document has no IANA actions.

9. References

9.1. Normative References

[FC-BGP-Protocol] Xu, K., Wang, X., liu, Z., Qi, L., Wu, J., and Y. Guo, "FC-BGP Protocol Specification", Work in Progress, Internet-Draft, draft-wang-sidrops-fcbgp-protocol-03, 6 April 2025, <https://datatracker.ietf.org/doc/html/draft-wang-sidrops-fcbgp-protocol-03>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

9.2. Informative References

[ASPP] McBride, M., Madory, D., Tantsura, J., Raszuk, R., Li, H., Heitz, J., and G. S. Mishra, "AS Path Prepending", Work in Progress, Internet-Draft, draft-ietf-grow-as-path-prepending-15, 23 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-as-path-prepending-15>.

[FC-ARXIV] "Secure Inter-domain Routing and Forwarding via Verifiable Forwarding Commitments", September 2023, <https://arxiv.org/abs/2309.13271>.

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <https://www.rfc-editor.org/rfc/rfc4272>.

[RFC5065] Traina, P., McPherson, D., and J. Scudder, "Autonomous System Confederations for BGP", RFC 5065, DOI 10.17487/RFC5065, August 2007, <https://www.rfc-editor.org/rfc/rfc5065>.

[RFC7132] Kent, S. and A. Chi, "Threat Model for BGP Path Security", RFC 7132, DOI 10.17487/RFC7132, February 2014, <https://www.rfc-editor.org/rfc/rfc7132>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Ke Xu
Tsinghua University
Beijing
China
Email: xuke@tsinghua.edu.cn

Xiaoliang Wang
Tsinghua University
Beijing
China
Email: wangxiaoliang0623@foxmail.com

Zhuotao Liu
Tsinghua University
Beijing
China
Email: zhuotaoliu@tsinghua.edu.cn

Qi Li
Tsinghua University
Beijing
China

Email: qli01@tsinghua.edu.cn

Jianping Wu
Tsinghua University
Beijing
China
Email: jianping@cernet.edu.cn

Ziwei Li
Zhongguancun Laboratory
Beijing
China
Email: lizw@zgclab.edu.cn

Yangfei Guo
Zhongguancun Laboratory
Beijing
China
Email: guoyangfei@zgclab.edu.cn