Spring Working Group
Internet-Draft
Intended status: Informational
Expires: 4 September 2025

Z. Du
China Mobile

3 March 2025

Encryption of SRv6 Function in SRv6 Network
draft-du-spring-srv6-function-encryption-00

Abstract

This document describes an encryption mechanism for the SRv6 function in the SRv6 nodes.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

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/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 September 2025.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

In [I-D.jliu-tpp-srv6], a trusted network path mechanism based on SRv6 is proposed to enable the path verification. To protect the path information, when forwarding a packet with an encrypted SRH header, each intermediate router needs to replace the source and destination filed of IPv6 Header with itself IPv6 address and its downstream router's IPv6 address and then forward it.

However, it is more straightforward that we still maintain the IPv6 header as usual, and just encrypt the function part of each SID. Thus, the attacker will only know where the packet would be forwarded to, and will not know what function would be executed in the next destination.

This document proposes an encryption mechanism for the SRH header to enhance the SRv6 security and protect the personal privacy in an SRv6 network.

2. Encrypting SRv6 Function

According to [RFC8986], an SRv6 SID can contain LOC, FUNCT, and ARG parts, where a locator (LOC) is routeable in the network, and the function (FUNCT) and arguments (ARG) will trigger the specific behavior on the corresponding node. The ARG can also be regarded as part of the FUNCT, which may or maynot appear in an SRv6 SID.

In this document, we suggest that we can encrypt the FUNCT part, and the ARG part if included. In the scenario, every node that supports the additional security of the function in the segment list, should have a key for the encryption. The encrypted SIDs should be marked, so that the node can decrypt the FUNCT part, and trigger the proper behavior.

A general procedure called option 1 in this document is described as follows:

1. The network element that makes up the SID list, for example the controller or the Headend node, should have the keys of the nodes along the path. When scheduling the SID list, the network element can encrypt the FUNCT part of an SID by using the key of the node related to the SID. Hence, the LOC part in the SID list is plaintext, and the FUNCT part is ciphertext. If the FUNCT part is encrypted, a flag should also be marked for it.

2. The Headend node sends out the packet containing the encrypted SID and the flag.

3. When an intermediate router receives the packet and the LOC part in the DA can be matched, it will see the flag and decrypt the FUNCT part. After that, the SID will be looked up in the SID table. The key should be the same as the one that is used to make up the SID.

4. The intermediate router executes the function, and if the current SID is not the last one, the intermediate router forwards the packet to the next destination.

Alternatively, we can also encrypt the LOC part of the next SID, so as to protect the path information. Another procedure called option 2 in this docuanment is described as follows:

1. The network element that makes up the SID list, for example the controller or the Headend node, should have the keys of the nodes along the path. When scheduling the SID list, the network element can encrypt the FUNCT part of an SID and the LOC part of the next SID if present by using the key of the node related to the current SID. Hence, the LOC part of the first SID is plaintext, the LOC part of the other SID is ciphertext, and the FUNCT part of all SIDs is ciphertext. If the FUNCT part is encrypted, a flag should be marked for it.

2. The Headend node sends out the packet containing the encrypted SID and the flag.

3. When an intermediate router receives the packet and the LOC part in the DA can be matched, it will see the flag and decrypt the FUNCT part, and the LOC part of the next SID if present. After that, the decrypted SID will be looked up in the SID table. The key used for the decryption should be the same as the the one that is used to make up the SID.

4. The intermediate router executes the function, and if the current SID is not the last one, the intermediate router forwards the packet to the next destination.

For the traditional mechanism, option 1, and option 2, three figures are shown as below.

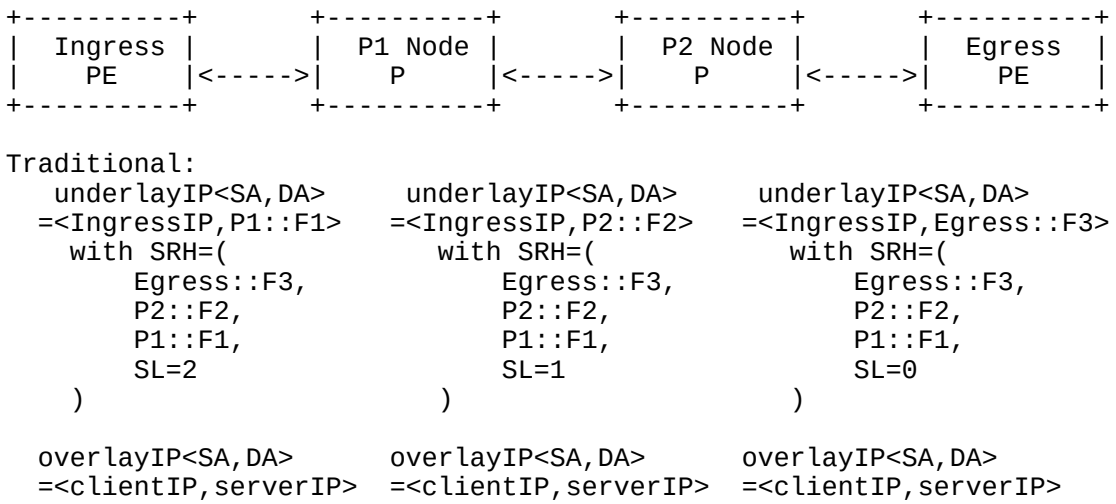

Figure 1: Traditional SRv6 Forwarding

In Figure 1, the packet from a client enters the provider network, and is encapsulated with another IP header with an SRH containing three SIDs. The Ingress PE is the Headend node, and the P1 and P2 nodes are the intermediate routers.

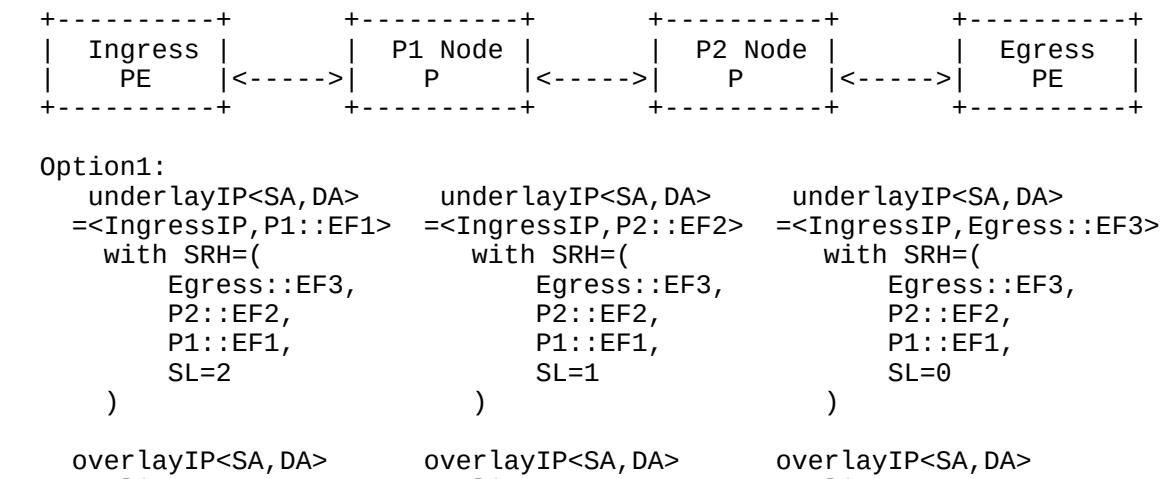

Figure 2: Encrypting SRv6 Function in Option 1

In Figure 2, the format of the packet is similar to the traditional one, but the function part is encrypted. For example, after the P1 node receives the EF1, it will be decrypted to F1, and then trigger the proper function.

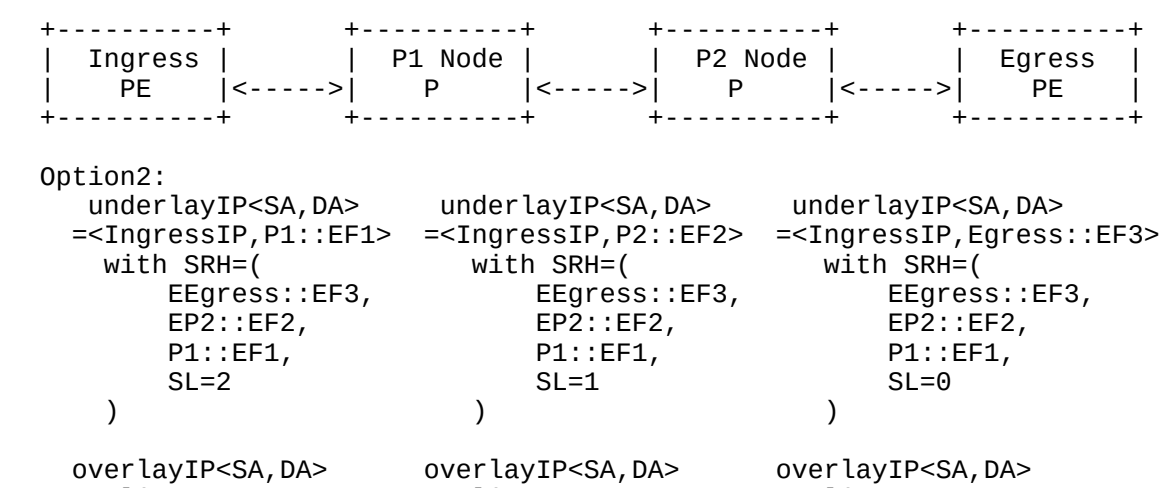

Figure 3: Encrypting SRv6 Function in Option 2

In Figure 3, the format of the packet is similar to the option 1. Additionally, the LOC part is also encrypted except the first SID. After the P1 node receives the EF1, it will be decrypted to F1, and

then trigger the proper function. Meanwhile, the P1 node will also decrypt the EP2 to P2, so as to make up the next DA as P2::EF2, which is routeable, instead of the EP2::EF2.

3. IANA Considerations

TBD.

4. Security Considerations

TBD.

5. Acknowledgements

TBD.

6. References

6.1. Normative References

[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/info/rfc2119>.

6.2. Informative References

[I-D.jliu-tpp-srv6] Liu, J., Li, H., Zhang, T., Wu, Q., and Z. Du, "A Path Verification Solution based on SRv6", Work in Progress, Internet-Draft, draft-jliu-tpp-srv6-00, 28 February 2024, <https://datatracker.ietf.org/doc/html/draft-jliu-tpp-srv6-00>.

[RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <https://www.rfc-editor.org/info/rfc8986>.

Author’s Address

Zongpeng Du
China Mobile
No.32 XuanWuMen West Street
Beijing
100053
China
Email: duzongpeng@foxmail.com